FULLY UPDATED
FOR THE NEW
3-PART CIA
EXAM

Wiley

CIAexcel

EXAM REVIEW 2014

PART 3 | INTERNAL AUDIT KNOWLEDGE ELEMENTS

S. Rao Vallabhaneni

WILEY

Wiley CIAexcel Exam Review 2014

Wiley CIAexcel Exam Review 2014

Part 3, Internal Audit Knowledge Elements

S. Rao Vallabhaneni

WILEY

Cover image: John Wiley & Sons, Inc.
Cover design: John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

ISBN 978-1-118-89359-3 (Paperback)
ISBN 978-1-118-96543-6
ISBN 978-1-118-96544-3
ISBN 978-1-118-89378-4 (Part 1)
ISBN 978-1-118-89355-5 (Part 2)
ISBN 978-1-118-89339-5 (Set)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The Certified Internal Auditor (CIA) Examination is a program of The Institute of Internal Auditors (IIA), Inc. The CIA Examination certifies a person as a professional internal auditor and is intended to measure the knowledge, skills, and competency required in the field of internal auditing. The CIA designation is the mark of an expert in internal auditing. The new exam syllabus, effective from the middle of 2013, tests knowledge at two levels of comprehension—proficiency and awareness, as indicated in the IIA's content specifications outlines (www.theiia.org). These levels require allocating more preparation time to proficiency-level topics and less time to awareness-level topics. The scope of the new CIA Exam consists of three parts, which are divided into 14 domains; there are three domains in Part 1, three domains in Part 2, and eight domains in Part 3.

A series of review books has been prepared for the candidate to utilize for all three parts of the new CIA Exam. Each part's review book includes a comprehensive coverage of the subject matter (theory) based on the new exam syllabus followed by some sample practice multiple-choice (M/C) questions with answers and explanations (practice). The sample practice M/C questions included in the review book are taken from Wiley's Web-based online test software to show you the flavor of the questions. Each part's review book contains a glossary section, which is a good source for answering M/C questions on the CIA Exam.

The scope of the Part 3 review book covers internal audit knowledge elements. It has eight domains: Domain 1 deals with governance and business ethics. Domain 2 addresses risk management. Domain 3 covers organizational structure, business processes, and risks. Domain 4 deals with communication. Domain 5 addresses management and leadership principles. Domain 6 focuses on information technology (IT) and business continuity. Domain 7 addresses financial management. Domain 8 focuses on global business environment. The Part 3 review book contains 140 sample practice M/C questions with answers and explanations, and a glossary section.

The objective of this review book is to provide single-source, comprehensive review materials to assist the CIA Exam candidate in successfully preparing for the exam. The major highlights are presented next.

- Easy to navigate, comprehend, learn, and apply the subject matter since it was written from a student's perspective in a textbook style and format.

- The review book contains fully developed theories and concepts with complete thoughts as opposed to mere outlines. The candidate needs to know more than outlines to pass the difficult CIA Exam.
- Each theoretical domain in the review book is shown with a range of percentages to indicate the relative weights given to that domain in the exam. Candidates are expected to plan their study time in proportion to the relative weights suggested (i.e., more time and effort to higher percentages, and vice versa).
- CIA Exam content specifications included at the beginning of the book shows the level of difficulty for each topic in the CIA Exam expressed as (A) for Awareness and (P) for Proficiency. Awareness means candidates must exhibit awareness (i.e., knowledge of terminology and fundamentals) in these topic areas. Proficiency means candidates must exhibit proficiency (i.e., thorough understanding and ability to apply concepts) in these topic areas.
- Greater use of comparisons and contrasts of subject matter make the key concepts come alive by providing lasting impressions. These comparisons show interrelationships between key concepts.

These review books focus on the student—the candidate preparing for the CIA exam. It provides a positive learning experience for candidates by helping them to remember what they read and recall the subject matter through the use of tree diagrams, line drawings, memory aids (key concepts to remember), tables, charts, and graphic text boxes. In other words, an attempt has been made to bring life to static words through visual aids and compare and contrast approaches (i.e., which is what). The positive learning experience system provided through visual aids and memories will enable candidates to form long-lasting study impressions of the subject matter in their minds. In short, this book is student-focused and learning-oriented.

The aim of these books is to make learning easier, more convenient, and more enjoyable for our customer, the student. A great deal of planning and thought went into the creation of these books with the single goal of making the student's study program (whether individual or group) more relevant and more meaningful. It is hoped that these books meet or exceed the student's expectations in terms of quality, content coverage, and presentation of the subject matter.

We were excited and challenged while writing these books, and we hope that you too will be excited to study, remember, and achieve lifelong benefit from them. We believe that the knowledge gained from these books will remain with the candidate even after passing the CIA Exam, serving as on-the-job reference material as well as a training source.

Our goal is to be responsive to the CIA Exam candidate's needs and provide customer (student) satisfaction through continuous quality improvement. This goal can be met only through timely feedback from the candidates. Please help us to serve you better—your input counts. You can reach us at ciatestbank@wiley.com.

Administrative Matters

We encourage the new, prospective candidate to obtain a copy of the CIA "Information for Candidates" brochure by writing directly to:

Institute of Internal Auditors

247 Maitland Avenue

Altamonte Springs, FL 32701-4201 USA

Phone: 407-937-1100, Fax: 407-937-1111

Web site: www.theiia.org

This brochure contains everything the candidate needs to know about the CIA Exam (i.e., application form, fees, dates, and sites).

Acknowledgments

The author is indebted to a number of people and organizations that helped to improve the content and quality of this book: Thanks to the Director of Certification at The Institute of Internal Auditors (IIA), Altamonte Springs, Florida, for providing great assistance during the writing of these books. Special thanks to the IIA for providing previous CIA Exam questions, answers, and explanations, IIA *Standards*, the Code of Ethics, and model exam questions. Many thanks also go to Wiley's editorial content management and marketing teams for their capable assistance in completing the CIA Exam learning system.

CIA Exam Study Preparation Resources

- To succeed in the exam, we recommend the following study plan and three review products for each part of the CIA Exam: Read the each part's review book (theory).
- Practice the Web-based online test bank software (practice).
- Reinforce the theoretical concepts by studying the Focus Notes (theory).

A series of review books have been prepared for the candidate to utilize for all three parts of the new CIA Exam. Each part's review book includes a comprehensive coverage of the subject matter (theory) followed by some sample practice multiple-choice (M/C) questions with answers and explanations (practice). The sample practice M/C questions included in the review book are taken from Wiley's Web-based online test software to show you the flavor of questions. Each part's review book contains a glossary section, which is a good source for answering M/C questions on the CIA Exam.

The **Web-based online test bank software** is a robust review product that simulates the format of the actual CIA Exam in terms of look and feel, thus providing intense practice and greater confidence to the CIA Exam candidates. The thousands of sample practice questions (5,275 plus) included in the online test bank can provide greater confidence and solid assurance to CIA exam candidates that they are preparing well for all the topics required and tested in the exam. All practice questions include explanations for the correct answer and are organized by domain topics within each part. See www.wileycia.com.

A part summary showing the number of sample practice questions included in the online test bank and the number of questions tested in the actual CIA Exam is presented next.

Part Summary	Wiley Sample Practice Questions	CIA Exam Actual Test Questions
Part 1	750+	125
Part 2	725+	100
Part 3	3,800+	100
Total Questions in Three Parts	**5,275+**	**325**

Focus Notes provide a quick review and reinforcement of the important theoretical concepts. They are presented in a summary manner taken from the details of the review books. The Focus Notes can be studied just before the exam, during travel time, or any other time. When combined, these three review products provide a great value to CIA Exam students.

We suggest a sequential study approach in four steps for each part of the exam, as follows:

Step 1. Read the glossary section at the end of each part's review book for a better understanding of key technical terms

Step 2. Study the theory from the each part's review book

Step 3. Practice the multiple-choice questions from the online test bank for each part

Step 4. Read the Focus Notes for each part for a quick review and reinforcement of the important theoretical concepts

In addition, the CIA Exam candidates should read **Practice Guides** from IIA because these guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, audit work programs, and step-by-step audit approaches as well as examples of audit deliverables. These Practice Guides are not included in the Wiley Review Books due to their size and the fact that they are available from www.theiia.org.

CIA Exam-Taking Tips and Techniques

The types of questions a candidate can expect to see in the CIA Exam are objective and scenario-based multiple-choice (M/C) questions. Answering the M/C questions requires a good amount of practice and effort.

The following tips and techniques will be helpful in answering the CIA Exam questions.

- Stay with your first impression of the correct choice.
- Know the subject area or topic. Don't read too much into the question.
- Remember that questions are independent of specific country, products, practices, vendors, hardware, software, or industry.
- Read the last sentence of the question first followed by all choices and then the body (stem) of the question.
- Read the question twice or read the bolded keywords twice, and watch for tip-off words, such as **not, except, all, every, always, never, least, or most,** which denote absolute conditions.
- Do not project the question into your organizational environment, practices, policies, procedures, standards, and guidelines. The examination is focusing on the IIA's professional *Standards* and publications and on the CIA's exam syllabus (i.e., content specifications).
- Try to eliminate wrong choices as quickly as possible. When you get down to two semifinal choices, take a big-picture approach. For example, if choice A and D are the semifinalists, and choice D could be a part of choice A, then select choice A; or if choice D could be a more complete answer, then select choice D.
- Don't spend too much time on one question. If you are not sure of an answer, move on, and go back to it if time permits. The last resort is to guess the answer. There is no penalty for guessing the wrong answer.

Remember that success in any professional examination depends on several factors required of any student, such as time management skills, preparation time and effort levels, education and experience levels, memory recall of the subject matter, state of the mind before or during the exam, and decision-making skills.

CIA Exam Content Specifications

Part 3 of the CIA Exam is called **internal audit knowledge elements** and the exam duration is 2.0 hours (120 minutes) with 100 multiple-choice questions. A breakdown of topics in the Part 3 follows.

Domain I: Governance and Business Ethics (5–15%)*

A. Corporate/Organizational Governance Principles (A) †

B. Business Ethics (A)

C. Corporate Social Responsibility (A)

Domain II: Risk Management (10–20%)

A. Risk Management Techniques (A)

B. Organizational Use of Risk Frameworks (A)

Domain III: Organizational Structure, Business Processes, and Risks (15–25%)

A. Risk/Control Implications of Different Organizational Structures (A)

B. Structure (e.g., centralized/decentralized) (A)

C. Typical Schemes in Various Business Cycles (e.g., procurement, sales, knowledge, and supply-chain management) (A)

D. Business Process Analysis (e.g., workflow analysis, bottleneck management, and Theory of Constraints) (A)

---

* Indicates the relative range of weights assigned to this topic area for both theory and practice sections in the CIA Exam.

† Indicates the level of difficulty for each topic in the CIA Exam expressed as (A) for Awareness and (P) for Proficiency. (A) = Candidates must exhibit awareness (i.e., knowledge of terminology and fundamentals) in these topic areas. (P) = Candidates must exhibit proficiency (i.e., thorough understanding and ability to apply concepts) in these topic areas.

E. Inventory Management Techniques and Concepts (A)

F. Electronic Funds Transfer and Electronic Data Interchange (EDI) (A)

G. Business Development Life Cycles ((A)

H. International Organization for Standardization Framework (A)

I. Outsourcing Business Processes (A)

Domain IV: Communication (5–10%)

A. Communication (e.g., the process, organizational dynamics, and impact of computerization) (A)

B. Stakeholder Relationships (A)

Domain V: Management and Leadership Principles (10–20%)

A. Strategic Management

- Forecasting (A)
- Quality management (e.g., TQM and Six Sigma) (A)
- Decision analysis (A)

B. Organizational Behavior

- Organizational theory (A)
- Organizational behavior (e.g., motivation, impact of job design, rewards, and schedules) (A)
- Group dynamics (e.g., traits, development stages, organizational politics, and effectiveness) (A)
- Knowledge of human resource processes (e.g., individual performance management, supervision, personnel sourcing/staffing, and staff development) (A)
- Risk/control implications of different leadership styles (A)

C. Management Skills

- Lead, inspire, and guide people, building organizational commitment and entrepreneurial orientation (A)
- Create group synergy in pursuing collective goals (A)

D. Conflict Management

- Conflict resolution (e.g., competitive, cooperative, and compromise) (A)
- Negotiation skills (A)
- Conflict management (A)
- Added-value negotiating (A)

E. Project Management and Change Management

- ☐ Change management (A)
- ☐ Project management techniques (A)

Domain VI: IT and Business Continuity (15–25%)

A. Security

- ☐ System security (e.g., firewalls and access controls) (A)
- ☐ Information protection (e.g., viruses and privacy) (A)
- ☐ Application authentication (A)
- ☐ Encryption (A)

B. Application Development

- ☐ End-user computing (A)
- ☐ Change control (A)
- ☐ Systems development methodology (A)
- ☐ Application development (A)
- ☐ Information systems development (A)

C. System Infrastructure

- ☐ Workstations (A)
- ☐ Databases (A)
- ☐ IT control frameworks (e.g., eSAC and COBIT) (A)
- ☐ Functional areas of IT operations (e.g., data center operations) (A)
- ☐ Enterprise-wide resource planning software (e.g., SAP R3) (A)
- ☐ Data and network communications and connections (e.g., LAN, VAN, and WAN) (A)
- ☐ Servers (A)
- ☐ Software licensing (A)
- ☐ Mainframe (A)
- ☐ Operating systems (A)

D. Business Continuity

- ☐ IT contingency planning (A)

Domain VII: Financial Management (13–23%)

A. Financial Accounting and Finance

- ☐ Basic concepts and underlying principles of financial accounting (e.g., statements, terminology, and relationships) (A)

- Intermediate concepts of financial accounting (e.g., bonds, leases, pensions, intangible assets, and research and development) (A)
- Advanced concepts of financial accounting (e.g., consolidation, partnerships, and foreign currency transactions) (A)
- Financial statement analysis (e.g., ratios) (A)
- Types of debt and equity (A)
- Financial instruments (e.g., derivatives) (A)
- Cash management (e.g., treasury functions) (A)
- Valuation models (A)
- Business valuation (A)
- Inventory valuation (A)
- Capital budgeting (e.g., cost of capital evaluation) (A)
- Taxation schemes (e.g., tax shelters and VAT) (A)

B. Managerial Accounting

- Managerial accounting: general concepts (A)
- Costing systems (e.g., activity-based and standard) (A)
- Cost concepts (e.g., absorption, variable, and fixed) (A)
- Relevant cost (A)
- Cost-volume-profit analysis (A)
- Transfer pricing (A)
- Responsibility accounting (A)
- Operating budget (A)

Domain VIII: Global Business Environment (0-10%)

A. Economic/Financial Environments (A)

B. Cultural/Political Environments (A)

C. Legal and Economics: General Concepts (A)

D. Impact of Government Legislation and Regulation on Business (e.g., Trade Legislation) (A)

DOMAIN 1

Governance and Business Ethics (5–15%)

1.1 Corporate/Organizational Governance Principles

The issue of corporate governance is a direct outgrowth of the question of legitimacy. For business to be legitimate and to maintain its legitimacy in the eyes of the public, its governance must correspond to the will of the people.

(a) What Is a Corporation?

(i) The Legal Entity

A corporation is a legal entity and is entitled to protection of the Fourteenth Amendment. In cases of piercing the corporate veil, courts have decided three things:

1. There was no right to pierce the veil for a personal injury victim.
2. There was a right to pierce the veil when a girl who drowned in a company's swimming pool would be compensated, saying that parent companies or shareholders would be treated as liable when they provide inadequate capitalization and actively participate in the conduct of corporate affairs.
3. There was no right to pierce the veil when insiders who become creditors of a company are subordinated to other creditors when the company becomes insolvent (known as the equitable principle or the Deep Rock doctrine).

(ii) Corporate Constitution

The essential elements of a corporate constitution include corporate charter (bylaws), director power and accountability (right to manage), and shareholder rights and duties (approve sale and purchase of company assets in a merger and acquisition). The purpose of a corporation may be anything that is lawful.

(b) What Is Corporate Governance?

The term "corporate governance" refers to the method by which a firm is being governed, directed, administered, or controlled and to the goals for which it is being governed. Corporate governance is concerned with the relative roles, rights, and accountability of such stakeholder groups as owners, boards of directors, managers, employees, labor unions, and others who assert to be stakeholders.

Corporate governance sets the right tone and proper stage for the entire corporation. While there is no standard definition of "corporate governance," it can broadly be understood to refer to the system by which companies are directed and controlled, including the role of the board of directors, management, shareholders, and other stakeholders. Corporate governance provides the structure through which the objectives of the company are set and the means of attaining those objectives and monitoring performance are determined.

A weak form of corporate governance is one of the root causes of many problems that corporate management faces today. Corporate governance and corporate ethics should support corporate management.

(c) Components of Corporate Governance

To appreciate fully the legitimacy and corporate governance issues, it is important to understand the major groups that make up the corporate form of business organization. Only by so doing can one appreciate how the system has failed to work according to its intended design.

The four major groups needed in setting the stage are (1) shareholders (owners or stakeholders), (2) board of directors, (3) managers, and (4) employees. Overarching these groups is the charter issued by the state, giving the corporation the right to exist and stipulating the basic terms of its existence.

Under U.S. corporate law, **shareholders** are the owners of a corporation. As owners, they should have ultimate control over the corporation. This control is manifested primarily in the right to select the board of directors of the company. Generally, the number of shares of stock owned determines the degree of each shareholder's right.

Because large organizations may have hundreds of thousands of shareholders, they elect a smaller group, known as the **board of directors**, to govern and oversee the management of the business. The board is responsible for ascertaining that the manager puts the interests of the owners (i.e., shareholders) first. The third major group in the authority hierarchy is **management**—the group of individuals hired by the board to run the company and manage it on a daily basis. Along with the board, top management establishes overall policy. Middle- and lower-level managers carry out this policy and conduct the daily supervision of the operative employees. **Employees** are those hired by the company to perform the actual operational work. Managers are employees too, but in this discussion we use the term "employees" to refer to nonmanagerial employees.

(d) Corporate Governance Problems

The major condition embedded in the structure of modern corporations that has contributed to the corporate governance problem has been the separation of ownership from control. In the precorporate period, owners typically were the managers themselves. As the public corporation grew and stock ownership became widely dispersed, a separation of ownership from control

became the prevalent condition. The shareholders were owners in a technical sense, but most of them perceived themselves to be investors rather than owners.

The other factors that added to management's power were the corporate laws and traditions that gave the management group control over the **proxy process**—the method by which the shareholders elected boards of directors. Over time, it was not difficult for management groups to create boards of directors of like-minded executives who would simply collect their fees and defer to management on whatever it wanted. The result of this process was that power, authority, and control began to flow upward from management rather than downward from the shareholders (owners). **Agency problems** developed when the interests of the shareholders were not aligned with the interests of the manager, and the manager (who is simply a hired **agent** with the responsibility of representing the owner's [principal's] best interest) began to pursue self-interest instead.

Market forces and agency costs aim to prevent or minimize agency problems. Examples of market forces include large shareholders and threat of takeover, where large institutional shareholders put pressure on company management to perform using their voting rights and where a constant threat of a takeover motivates company management to act in the best interest of the corporation owners. Examples of agency costs include (1) cost of management compensation in terms of incentive plans (stock options), performance plans (performance shares), and cash bonuses; and (2) costs imposed by lenders (creditors and bankers) in the form of constraints put on the borrower's actions to protect the lenders' investment (e.g., minimum liquidity levels, merger and acquisition activities, executive salaries, and dividend payments).

(e) Corporate Governance Standards

Business Roundtable supports eight guiding principles and standards as part of good corporate governance practices.[1]

1. The paramount duty of the board of directors of a public corporation is to select a chief executive officer [CEO] and to oversee the CEO and senior management in the competent and ethical operation of the corporation on a day-to-day basis.
2. It is the responsibility of management to operate the corporation in an effective and ethical manner to produce value for shareholders. Senior management is expected to know how the corporation earns its income and what risks the corporation is undertaking in the course of carrying out its business. The CEO and board of directors should set a "tone at the top" that establishes a culture of legal compliance and integrity. Management and directors should never put personal interests ahead of or in conflict with the interests of the corporation.
3. It is the responsibility of management, under the oversight of the audit committee and the board, to produce financial statements that fairly present the financial condition and results of operations of the corporation and to make the timely disclosures investors need to assess the financial and business soundness and risks of the corporation.
4. It is the responsibility of the board, through its audit committee, to engage an independent accounting firm to audit the financial statements prepared by management, issue an opinion that those statements are fairly stated in accordance with generally accepted accounting principles (GAAP) and oversee the corporation's relationship with the outside auditor.

[1] Business Roundtable, *Principles of Corporate Governance*, pp. 2–3, 2005, Washington, DC.

5. It is the responsibility of the board, through its corporate governance committee, to play a leadership role in shaping the corporate governance of the corporation. The corporate governance committee also should select and recommend to the board qualified director candidate for election by the corporation's shareholders.
6. It is the responsibility of the board, through its compensation committee, to adopt and oversee the implementation of compensation policies, establish goals for performance-based compensation, and determine the compensation of the CEO and senior management.
7. It is the responsibility of the board to respond appropriately to shareholder's concerns.
8. It is the responsibility of the corporation to deal with its employees, customers, suppliers, and other constituencies in a fair and equitable manner.

These eight responsibilities and others are critical to the functioning of the modern public corporation and the integrity of the public markets. No law or regulation alone can be a substitute for the voluntary adherence to these principles by corporate directors and management.

Business Roundtable believes that corporate governance should be enhanced through conscientious and forward-looking action by a business community that focuses on generating long-term shareholder value with the highest degree of integrity.

The principles discussed here are intended to assist corporate management and boards of directors in their individual efforts to implement best practices of corporate governance as well as to serve as guideposts for the public dialogue on evolving governance standards.

(f) Corporate Governance Principles

Since 1999, the Organisation for Economic Co-operation and Development (OECD) *Principles of Corporate Governance* has become an international benchmark for policy makers, investors, corporations, and other stakeholders worldwide. The OECD, located in Paris, France, consists of 30 member countries with policies aimed at improving economic growth and employment, world economy, and world trade. The OECD has developed six principles of corporate governance.[2]

(i) Principle I: Ensuring the Basis for an Effective Corporate Governance Framework

The corporate governance framework should promote transparent and efficient markets, be consistent with the rule of law, and clearly articulate the division of responsibilities among different supervisory, regulatory, and enforcement authorities.

- The corporate governance framework should be developed with a view to its impact on overall economic performance, market integrity, and the incentives it creates for market participants and the promotion of transparent and efficient markets.
- The legal and regulatory requirements that affect corporate governance practices in a jurisdiction should be consistent with the rule of law, transparent, and enforceable.

[2] OECD *Principles of Corporate Governance* (Paris, France: OECD, 2004), pp. 17–25. http://www.oecd.org/daf/corporateaffairs/corporategovernanceprinciples/31557724.pdf

- The division of responsibilities among different authorities in a jurisdiction should be clearly articulated, and ensure that the public interest is served.
- Supervisory, regulatory, and enforcement authorities should have the authority, integrity, and resources to fulfill their duties in a professional and objective manner. Moreover, their rulings should be timely, transparent, and fully explained.

(ii) Principle II: Rights of Shareholders and Key Ownership Functions

The corporate governance framework should protect and facilitate the exercise of shareholders' rights.

- Basic shareholder rights should include the rights to:
  1. Secure methods of ownership registration.
  2. Convey or transfer shares.
  3. Obtain relevant and material information on the corporation on a timely and regular basis.
  4. Participate and vote in general shareholder meetings.
  5. Elect and remove members of the board.
  6. Share in the profits of the corporation.
- Shareholders should have the right to participate in, and to be sufficiently informed on, decisions concerning fundamental corporate changes, such as (1) amendments to the statutes, articles of incorporation, or similar governing documents of the company; (2) the authorization of additional shares; and (3) extraordinary transactions, including the transfer of all or substantially all assets, that in effect result in the sale of the company.
- Shareholders should have the opportunity to participate effectively and vote in general shareholder meetings and should be informed of the rules, including voting procedures, that govern shareholder meetings.
  - Shareholders should be furnished with sufficient and timely information concerning the date, location, and agenda of general meetings as well as full and timely information regarding the issues to be decided at the meeting.
  - Shareholders should have the opportunity to ask questions to the board, including questions relating to the annual external audit, to place items on the agenda of general meetings, and to propose resolutions, subject to reasonable limitations.
  - Effective shareholder participation in key corporate governance decisions, such as the nomination and election of board members, should be facilitated. Shareholders should be able to make their views known on the remuneration policy for board members and key executives. The equity component of compensation schemes for board members and employees should be subject to shareholder approval.
  - Shareholders should be able to vote in person or in absentia, and equal effect should be given to votes whether cast in person or in absentia.
- Capital structures and arrangements that enable certain shareholders to obtain a degree of control disproportionate to their equity ownership should be disclosed.
- Markets for corporate control should be allowed to function in an efficient and transparent manner.

- The rules and procedures governing the acquisition of corporate control in the capital markets and extraordinary transactions, such as mergers and sales of substantial portions of corporate assets, should be clearly articulated and disclosed so that investors understand their rights and recourse. Transactions should occur at transparent prices and under fair conditions that protect the rights of all shareholders according to their class.
- Antitakeover devices should not be used to shield management and the board from accountability.

- The exercise of ownership rights by all shareholders, including institutional investors, should be facilitated.
  - Institutional investors acting in a fiduciary capacity should disclose their overall corporate governance and voting policies with respect to their investments, including the procedures that they have in place for deciding on the use of their voting rights.
  - Institutional investors acting in a fiduciary capacity should disclose how they manage material conflicts of interest that may affect the exercise of key ownership rights regarding their investments.
- Shareholders, including institutional shareholders, should be allowed to consult with each other on issues concerning their basic shareholder rights as defined in the *Principles*, subject to exceptions to prevent abuse.

(iii) Principle III: Equitable Treatment of Shareholders

The corporate governance framework should ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights.

- All shareholders of the same series of a class should be treated equally.
  - Within any series of a class, all shares should carry the same rights. All investors should be able to obtain information about the rights attached to all series and classes of shares before they purchase. Any changes in voting rights should be subject to approval by those classes of shares that are negatively affected.
  - Minority shareholders should be protected from abusive actions by, or in the interest of, controlling shareholders acting either directly or indirectly and should have effective means of redress.
  - Votes should be cast by custodians or nominees in a manner agreed upon with the beneficial owner of the shares.
  - Impediments to cross border voting should be eliminated.
  - Processes and procedures for general shareholder meetings should allow for equitable treatment of all shareholders. Company procedures should not make it unduly difficult or expensive to cast votes.
- Insider trading and abusive self-dealing should be prohibited.
- Members of the board and key executives should be required to disclose to the board whether they directly, indirectly, or on behalf of third parties have a material interest in any transaction or matter directly affecting the corporation.

(iv) Principle IV: Role of Stakeholders in Corporate Governance

The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active cooperation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

- The rights of stakeholders that are established by law or through mutual agreements are to be respected.
- Where stakeholder interests are protected by law, stakeholders should have the opportunity to obtain effective redress for violation of their rights.
- Performance-enhancing mechanisms for employee participation should be permitted to develop.
- Where stakeholders participate in the corporate governance process, they should have access to relevant, sufficient, and reliable information on a timely and regular basis.
- Stakeholders, including individual employees and their representative bodies, should be able to freely communicate their concerns about illegal or unethical practices to the board and their rights should not be compromised for doing this.
- The corporate governance framework should be complemented by an effective, efficient insolvency framework and by effective enforcement of creditor rights.

(v) Principle V: Disclosure and Transparency

The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company.

- Disclosure should include, but not be limited to, material information on:
  - The financial and operating results of the company.
  - Company objectives.
  - Major share ownership and voting rights.
  - Remuneration policy for members of the board and key executives, and information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.
  - Related party transactions.
  - Foreseeable risk factors.
  - Issues regarding employees and other stakeholders.
  - Governance structures and policies, in particular, the content of any corporate governance code or policy and the process by which it is implemented.
- Information should be prepared and disclosed in accordance with high-quality standards of accounting and financial and nonfinancial disclosure.
- An annual audit should be conducted by an independent, competent, and qualified auditor in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company in all material respects.

- External auditors (EAs) should be accountable to the shareholders and owe a duty to the company to exercise due professional care in the conduct of the audit.
- Channels for disseminating information should provide for equal, timely, and cost-efficient access to relevant information by users.
- The corporate governance framework should be complemented by an effective approach that addresses and promotes the provision of analysis or advice by analysts, brokers, credit rating agencies (CRAs), and others that is relevant to decisions by investors, free from material conflicts of interest that might compromise the integrity of their analysis or advice.

(vi) Principle VI: Responsibilities of the Board

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.

- Board members should act on a fully informed basis, in good faith, with due diligence and care, and in the best interest of the company and the shareholders.
- Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.
- The board should apply high ethical standards. It should take into account the interests of stakeholders.

SUMMARY OF BOARD OF DIRECTORS' DUTIES

Board of directors have three fiduciary duties: (1) duty of care (i.e., business judgment rule), (2) self-dealing (i.e., fair to the company), and (3) corporate opportunities (e.g., mergers, acquisitions, and divestitures).

The business judgment rule is a legal presumption that the directors and officers of the corporation have exercised **duty of care** by acting on an informed basis, in good faith, and in the honest belief that their actions are in the best interests of the corporation. Unless a plaintiff can give persuasive evidence against at least one of the criteria, corporate directors and officers are insulated from liability for breach of the duty of care.

Regarding **self-dealing**, corporate directors and officers may pursue business transactions that benefit themselves as long as they can prove that the transaction, although self-interested, was nevertheless intrinsically fair to the corporation (i.e., the transaction is initiated and completed at an arm's-length distance). A plaintiff must start by alleging the director or officer stood to gain a material economic benefit. The burden then shifts to the defendant to show the fairness of the transaction. The court considers both the terms and the process for the bargain (i.e., both a fair price and fair dealing). However, if the director shows that full disclosure was made to disinterested directors or disinterested shareholders, then the burden remains on the plaintiff.

As a part of fiduciary duties, it is acceptable for directors to inform one another of **corporate opportunities** that arise. Examples of these opportunities include identifying candidates for mergers, acquisitions, and divestitures; introducing new products, new suppliers, new customers, new contractors, new technologies, and new business ventures; and bringing awareness of new laws and regulations.

- The board should fulfill certain key functions, including:
  - Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budget, and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions, and divestitures.
  - Monitoring the effectiveness of the company's governance practices and making changes as needed.
  - Selecting, compensating, monitoring, and, when necessary, replacing key executives and overseeing succession planning.
  - Aligning key executive and board remuneration with the longer-term interests of the company and its shareholders.
  - Ensuring a formal and transparent board nomination and election process.
  - Monitoring and managing potential conflicts of interest of management, board members, and shareholders, including misuse of corporate assets and abuse in related party transactions.
  - Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place—in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.
  - Overseeing the process of disclosure and communication.
- The board should be able to exercise objective independent judgment on corporate affairs.
  - Boards should consider assigning a sufficient number of nonexecutive board members capable of exercising independent judgment to tasks where there is a potential for conflict of interest. Examples of such key responsibilities are ensuring the integrity of financial and nonfinancial reporting, the review of related party transactions, nomination of board members and key executives, and board remuneration.
  - When committees of the board are established, their mandate, composition, and working procedures should be well defined and disclosed by the board.
  - Board members should be able to commit themselves effectively to their responsibilities.
- In order to fulfill their responsibilities, board members should have access to accurate, relevant, and timely information.

(g) Need for Board Independence

Board independence from management is a crucial aspect of good corporate governance. It is here that the difference between inside directors and outside directors is most pronounced. Outside directors are independent from the firm and its top managers. In contrast, inside directors have some sort of ties to the firm. Sometimes they are top managers in the firm; other times insiders are family members or others with close ties to the CEO. To varying degrees, each of these parties is beholden to the CEO and, therefore, might be hesitant to speak out when necessary.

Another problem is managerial control of the board processes. CEOs often can control board perquisites (perks), such as director compensation and committee assignments. Board members who rock the boat may find they are left out in the cold. Two issues surrounding compensation

include (1) CEO compensation, which is very controversial, and (2) director compensation, which is very subjective or can be interpreted as self-dealing.

(h) Insider Trading Scandals

Insider trading is the practice of obtaining critical information from inside a company and then using that information for one's own personal financial gain. Not only are shareholders suspicious of what has been going on unbeknownst to them, but small investors and the general public have lost faith in what they thought was the stable and secure financial industry. When companies disclose meaningful information to shareholders and securities professionals, they must do so publicly so that small investors can enjoy a more level playing field.

(i) Board Member Liabilities

In the mid- to late 1980s, not many individuals wanted board director positions. Concerned about increasing legal hassles emanating from stockholder, customer, and employee lawsuits, directors were quitting such positions or refusing to accept them. Although courts rarely hold directors personally liable in the hundreds of shareholder suits filed every year, over the past several years, there have been a few cases in which directors have been held personally and financially liable for their decisions.

The Private Securities Litigation Reform Act of 1995 made it more difficult for shareholders to bring class action lawsuits to federal courts. However, rather than stemming the tide of lawsuits, the act simply prompted shareholders to change their venue. Suits filed in federal courts decreased while suits filed in state courts increased. The Securities Litigation Uniform Standards Act of 1998 was designed to plug that loophole. This act says: "Any covered class action suit brought into any state courts shall be removable to the federal district courts for the district in which the action is pending."

(j) Improving Corporate Governance

Efforts to improve corporate governance may be classified into two major categories: (1) changes could be made in the composition, structure, and functioning of boards of directors; and (2) shareholders—on their own initiative or on the initiative of management or the board—could assume a more active role in governance.

Specifically, improving corporate governance requires four things:

1. Increased change in the composition of the directors between inside directors and outside directors
2. Increased role of shareholders with their initiatives to companies
3. Increased role of company initiatives to shareholders
4. Increased obligation of companies to fully disclose vital information to shareholders

(k) Global Practices in Corporate Governance

Corporate governance practices differ considerably around the globe. although there are some common practices. Regardless, most corporate governance problems are rooted in three areas: (1) poor governance policies and practices, (2) fraudulent accounting practices, and (3) executives'

excessive and abusive behavior. Specific issues deal with ownership, board composition, influence, power, and control, as follows:

- Ownership is heavily dispersed in the United States but is much more concentrated in Canada, Germany, Japan, and China. High levels of influence and control over corporate affairs are associated with high concentration of ownership.
- National and state governments also own major stakes of public companies in Germany, Japan, and China.
- French and German companies have different types of owners than those found in the United States and United Kingdom. In France, nonfinancial corporations and state government are the largest shareholders. In Germany, both banks and nonfinancial corporations are owners. In addition, German banks own both debt and equity in the same corporation; they have direct voting power and proxy voting positions from bank depositors.
- Most shares of Chinese public firms are controlled by state-owned or state-controlled shareholders. The remaining trading shares are owned by a combination of individual and institutional investors.
- In Brazil, China, France, and Russia, the government owns the largest companies.
- Owners and workers sit on the board in France, Germany, Japan, and China. Outsiders and managers sit on the board in U.S., U.K., and Canadian companies.
- CEOs have considerable power over the selection of board members in many U.S. corporations as well as in Canada and the United Kingdom. In France and Germany, owners nominate and elect the board members.

(I) Roles of the Board of Directors

An effective system of corporate governance provides the framework within which the board and management address their respective responsibilities.[3]

- The business of a corporation is managed under the direction of the corporation's board. The board delegates to the CEO—and through the CEO to other senior management—the authority and responsibility for managing the everyday affairs of the corporation. Directors monitor management on behalf of the corporation's shareholders.
- Making decisions regarding the selection, compensation, and evaluation of a well-qualified and ethical CEO is the single most important function of the board. The board also appoints or approves other members of the senior management team.
- Directors bring to the corporation a range of experience, knowledge, and judgment. Directors should not represent the interests of particular constituencies.
- Effective directors maintain an attitude of constructive skepticism; they ask incisive, probing questions and require accurate, honest answers; they act with integrity and diligence; and they demonstrate a commitment to the corporation, its business plans, and long-term shareholder value.
- In performing its oversight function, the board is entitled to rely on the advice, reports, and opinions of management, corporate counsel, auditors, and expert advisors. The board should assess the qualifications of those it relies on and hold managers and advisers accountable.

[3] Business Roundtable, *Principles of Corporate Governance*, pp. 7–10 .

The board should ask questions and obtain answers about the processes used by managers and the corporation's advisors to reach their decisions and recommendations as well as about the substance of the advice and reports received by the board. When appropriate, the board and its committees should seek independent advice.

ROLES OF THE BOARD OF DIRECTORS

The roles of the board of directors can be described in terms of six topics: (1) monitoring of management; (2) due care, duty of due care, due diligence, and duty of loyalty; (3) ethical standards; (4) key functions; (5) corporate affairs; and (6) access to information.

- Given the board's oversight role, shareholders and other constituencies can reasonably expect that directors will exercise vigorous and diligent oversight of a corporation's affairs. However, they should not expect the board to micromanage the corporation's business by performing or duplicating the tasks of the CEO and senior management team.
- The board's oversight function carries with it a number of specific responsibilities in addition to that of selecting and overseeing the CEO. These responsibilities include:

  a. **Planning for management development and succession.** The board should oversee the corporation's plans for developing senior management personnel and plan for CEO and senior management succession. When appropriate, the board should replace the CEO or other members of senior management.

  b. **Understanding, reviewing, and monitoring the implementation of the corporation's strategic plans.** The board has responsibility for overseeing and understanding the corporation's strategic plans from their inception through their development and execution by management. Once the board reviews a strategic plan, it should regularly monitor implementation of the plan to determine whether it is being implemented effectively and whether changes are needed. The board also should ensure that the corporation's incentive compensation program is aligned with the corporation's strategic plan.

  c. **Understanding and approving annual operating plans and budgets.** The board is responsible for understanding, approving, and overseeing the corporation's annual operating plans and for reviewing the annual budgets presented by management. The board should monitor implementation of the annual plans to assess whether they are being implemented effectively and within the limits of approved budgets.

  d. **Focusing on the integrity and clarity of the corporation's financial statements and financial reporting.** The board, assisted by its audit committee, should be satisfied that the financial statements and other disclosures prepared by management accurately present the corporation's financial condition and results of operations to shareholders and that they do so in an understandable manner. To achieve accuracy and clarity, the board, through its audit committee, should have an understanding of the corporation's financial statements, including why the accounting principles critical to the corporation's business were chosen, what key judgments and estimates were made by management, and how the choice of principles and the making of these judgments and estimates affect the reported financial results of the corporation.

  e. **Advising management on significant issues facing the corporation.** Directors can offer management a wealth of experience and a wide range of perspectives. They provide advice and counsel to management in formal board and committee meetings, and they are available for informal consultation with the CEO and senior management.

f. **Reviewing and approving significant corporate actions.** As required by state corporate law, the board reviews and approves specific corporate actions, such as the election of executive officers, the declaration of dividends and (as appropriate) the implementation of major transactions. The board and senior management should have a clear understanding of what level or types of decisions require specific board approval.

g. **Reviewing management's plans for business resiliency.** As part of its oversight function, the board should designate senior management who will be responsible for business resiliency. The board should periodically review management's plans to address this issue. Business resiliency can include such items as business risk assessment and management, business continuity, physical and cybersecurity, and emergency communications.

h. **Nominating directors and committee members and overseeing effective corporate governance.** It is the responsibility of the board, through its corporate governance committee, to nominate directors and committee members and oversee the composition, independence, structure, practices, and evaluation of the board and its committees.

i. **Overseeing legal and ethical compliance.** The board should set a tone at the top that establishes the corporation's commitment to integrity and legal compliance. The board should oversee the corporation's compliance program relating to legal and ethical conduct. In this regard, the board should be knowledgeable about the corporation's compliance program and should be satisfied that the program is effective in preventing and deterring violations. The board should pay particular attention to conflicts of interest, including related party transactions.

(m) Roles of Chief Executive Officers and Senior Executives

Business Roundtable defines the following specific roles and responsibilities for CEOs and other senior executives.[4]

1. It is the responsibility of the CEO and senior management (senior executives), under the CEO's direction, to operate the corporation in an effective and ethical manner. As part of its operational responsibility, senior management is charged with the following tasks:

   a. **Operating the corporation.** The CEO and senior management runs the corporation's day-to-day business operations. With a thorough understanding of how the corporation operates and earns its income, they carry out the corporation's strategic objectives within the annual operating plans and budgets, which are reviewed and approved by the board. In making decisions about the corporation's business operations, the CEO considers the long-term interests of the corporation and its shareholders and necessarily relies on the input and advice of others, including senior management and outside advisors. The CEO keeps the board apprised of significant developments regarding the corporation's business operations.

   b. **Strategic planning.** The CEO and senior management generally takes the lead in strategic planning. They identify and develop strategic plans for the corporation; present those plans to the board; implement the plans once board review is completed; and recommend and carry out changes to the plans as necessary.

   c. **Annual operating plans and budgets.** With the corporation's overall strategic plans in mind, senior management develops annual operating plans and budgets for the corporation and presents the plans and budgets to the board. Once the board has

[4] Ibid., pp. 10–12.

reviewed and approved the plans and budgets, the management team implements the annual operating plans and budgets.

d. **Selecting qualified management and establishing an effective organizational structure.** Senior management is responsible for selecting qualified management and implementing an organizational structure that is efficient and appropriate for the corporation's particular circumstances.

e. **Identifying and managing risk.** Senior management identifies and manages the risks that the corporation undertakes in the course of carrying out its business. It also manages the corporation's overall risk profile.

f. **Accurate and transparent financial reporting and disclosures.** Senior management is responsible for the integrity of the corporation's financial reporting system and the accurate and timely preparation of the corporation's financial statements and related disclosures in accordance with GAAP and in compliance with applicable laws and regulations. It is senior management's responsibility—under the direction of the CEO and the chief financial officer (CFO)— to establish, maintain, and periodically evaluate the corporation's internal controls and procedures. In accordance with applicable laws and regulations, the CEO and the CFO also are responsible for certifying the accuracy and completeness of the corporation's financial statements and the effectiveness of the corporation's internal and disclosure controls.

ROLES OF THE CHIEF EXECUTIVE OFFICER

The CEO's management style, tone, and leadership skills set the stage for the entire corporation, which determines the ultimate success or failure of the organization. The CEO is the linchpin to the strategic management process in setting the overall direction for the organization and mobilizing resources to accomplish the organization mission, vision, goals, and objectives.

Along with the CFO, the CEO is the contact person for the stock markets, investment analysts, and the media in communicating financial and operational performance results. The CEO possesses more soft skills than hard skills. The management style and leadership skills of other senior executives should be compatible with those of the CEO to ensure goal congruence.

2. The CEO and senior management are responsible for operating the corporation in an ethical manner. They should never put individual, personal interests before those of the corporation or its shareholders. Business Roundtable believes that when carrying out this function, corporations should have three elements in place:

   a. **CEO of Integrity.** The CEO should be a person of integrity who takes responsibility for the corporation adhering to the highest ethical standards.

   b. **Strong, ethical tone at the top.** The CEO and senior management should set a tone at the top that establishes a culture of legal compliance and integrity communicated to personnel at all levels of the corporation.

   c. **Effective compliance program.** Senior management should take responsibility for implementing and managing an effective compliance program relating to legal and ethical conduct. As part of its compliance program, a corporation should have a code of conduct with effective reporting and enforcement mechanisms. Employees should have a means of seeking guidance and alerting management and the board about potential or actual misconduct without fear of retribution, and violations of the code should be addressed promptly and effectively.

(n) Roles and Responsibilities of the Chief Governance Officer

The overall role of the chief governance officer (CGO) is to promote good corporate governance practices. The CGO position must be a permanent one, not a temporary job created to handle a corporate crisis situation. Stakeholders will invite the permanent establishment of a CGO position since it sends a positive signal to the capital markets. This good news, in turn, increases the market price of a company's stock and lowers the cost of capital for the company. As with any other sensitive position, the corporation's internal environment, consisting of directors and management, must be supportive of good governance principles and in the hiring and functioning of a CGO job. In order to fulfill the roles and responsibilities, the CGO should have a free and full access to all board members and the chairperson of the board.

Specifically, these are the roles and responsibilities of a CGO:

- Establish the goals of good corporate governance, addressing board oversight, exacting ethical behavior, creating trust, and hiring competent management.
- Make corporate board members and management accountable for their actions.
- Develop governance principles, policies, and practices, covering the composition of the board; qualities of nonmanagement (nonexecutive) directors; composition and responsibilities of various committees; and allocation and balance of power among the owners, management, and the board.
- Communicate freely and fully about governance principles and policies both inside and outside of the organization.
- Notify government regulators and authorities through periodic filings to them about the governance accomplishments. Do the same thing with the general public through news media.
- Provide training to management and nonmanagement employees of the organization about good governance principles, policies, and practices,
- Seek out best practices in corporate governance that other organizations implemented through benchmarking.
- Reexamine and reevaluate governance principles, policies, and practices, and update them as needed on an ongoing basis.
- Conduct governance audits, management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in corporate governance practices.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnects between these views and to integrate them in a coherent manner.

(o) Roles and Responsibilities of the Audit Committee

(i) Overview

Vibrant and stable capital markets depend on, among other things, reliable, transparent, and objective financial information to support an efficient and effective capital allocation process. The vital oversight role audit committees play in the process of producing financial information has never been more important. As the capital markets continue to digest

various corporate governance reforms, audit committees have been forced to refine—some would say redefine—their mission. And with these changes, the natural tension between the board's dual roles as an advisor to management and a fiduciary to shareholders is heightened, with audit committee often at the center of the tension. Quite fundamentally, the capital market system today expects more from an audit committee than it ever has. How audit committees react to these changing expectations is a key factor in restoring credibility in financial information.[5]

The audit committee's key responsibility—overseeing the process that produces reliable and credible financial statements while ensuring the company has effective internal controls—requires it to conduct activities that previously had been executed mostly by management. Today audit committees are also expected to retain and compensate the EAs, grasp all of the key information included in a company's financial reporting, and oversee risk management and compliance with the laws and regulations affecting the company. This change is occurring in an environment that demands transparency.

(ii) Charter and Evaluation

Charters—the clearest articulation of the audit committee's purpose, composition, roles and responsibilities, and authority—are public documents. That makes it even more important for committees to evaluate regularly whether their charters are appropriate and whether they are discharging all their responsibilities. Committee evaluations, useful in identifying areas for improvement and training needs, raise new concerns over putting results in writing.

(iii) Financial Statements

In today's world, financial statements are extremely dense and, too often, difficult to understand. Indeed, they are so complicated that many audit committees struggle to grasp them or to feel completely confident they portray business results in the most effective way, particularly in areas where the accounting is highly technical and complex. Although many individual investors do not read the full financial statements, that does not diminish the importance of the audit committee's role in ensuring they are understandable and transparent for those companies and individuals who do. Audit committees can bring the discipline to ensure that companies provide digestible and reliable information to the investor world.

(iv) Risk Management and Internal Control

When people talk about risk, they often mean different things—such as insurance or hedging, or regulatory, product, or technology risk. While audit committees long have overseen how companies respond to financial reporting risks, some now are overseeing the effectiveness of management's responses to additional types of risk, the kinds outlined earlier as well as other risks that might prevent a company from achieving its strategic objectives. It is vital that the board agrees up front on the scope of the audit committee's oversight, so the board can ensure all key risks are monitored somewhere at the board level. Then the audit committee needs to understand those risks within its purview and be confident that management's responses—the internal controls it has established and operate—are satisfactory and that management's process for identifying and assessing risk is sound. In the same way that the audit committee should ensure proper transparency of the financial statements, it also should

[5] *Audit Committee Effectiveness: What Works Best*, 3rd ed. (Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 2005).

ensure that management's reporting on the effectiveness of internal control over financial reporting is complete and understandable.

(v) Oversight of Management and Internal Audit

Audit committees always have needed to balance their fiduciary role with their role as advisors to management. However, as audit committee responsibilities have increased and the external pressure to emphasize their fiduciary role mounts—questioning and pressing management more, trusting less—tensions naturally increase.

RESPONSIBILITIES OF THE AUDIT COMMITTEE AND ITS RELATIONSHIP WITH CORPORATE MANAGEMENT

The principal responsibilities of an audit committee are to:

- Ensure that published financial statements are not misleading.
- Ensure that internal controls are adequate.
- Follow up on allegations of material, financial, ethical, and legal irregularities.
- Ratify the selection of the EA.

Regarding relationships, audit committees should press corporate management more and trust it less.

Of course, audit committees must evaluate whether what management is telling them is supportable. Many audit committees look to the internal audit function for that insight and rely on internal audit's objective assessment of risk and control in operational, compliance, and reporting areas. Audit committees should consider whether the internal audit function has the proper stature in the company. The audit committee will benefit, and it is in the committee's self-interest to be internal audit function's champion.

(vi) Relationship with External Auditors

EAs play one of the key gatekeeper roles in the capital markets. Audit committees should own the relationship with the external auditors—if they do not and it is evident management still does, they need to take immediate steps to own it. Audit committees "owning" the relationship have direct reporting by EAs, ongoing communication, frequent meetings, and robust discussions about audit scope and audit results. They pay more attention to greater levels of detail, evaluating potential services to determine whether the committee will grant its preapproval, taking steps to ensure the auditors' independence, and considering how well the auditors perform.

(vii) Compliance and Ethics

Witnessing how quickly corporate and personal reputations can be destroyed has provided a wake-up call for many directors. They recognize that, often, the greatest harm is caused by an individual's unethical actions. Therefore, ethics, codes of conduct, and tone at the top are vital in protecting a company against reputation risk. While failing to comply with legal and regulatory requirements may be driven by carelessness to process problems—more neglect than outright malfeasance—to the outside world, such lack of compliance simply looks as if the company does not care enough about compliance to focus on it, which again affects reputation. Many audit committees are playing a central role in addressing the evolving regulatory expectations for board-level involvement in compliance and ethics.

(viii) Committee Composition

Requirements for independence and financial literacy, limitations on the number of audit committees on which a director can serve, and concerns around liability have made it more challenging to recruit qualified members to an audit committee. The significant workload and time commitment required of audit committee members may be responsible for shifting committee composition, with active board chairs, CEOs, and presidents constituting a smaller portion of committee membership than they did in the past.

(ix) Meetings Agenda

Audit committees have to steer their agenda—not abdicating their responsibility to management. Audit committee chairs often provide the foundation for effective audit committee meetings—driving the agenda, facilitating the discussion, holding premeetings to explore issues, and ensuring the right people are present. Audit committee members also must prepare thoroughly for meetings. And the meetings need to have active meaningful participation, not presentation, sometimes requiring presenters be coached in advance of meetings.

(x) Training

With the intricate nature of companies' business activities, the complexity of accounting transactions and policies, and frequent changes to financial accounting standards, even the most experienced audit committee members can benefit from training. New audit committee members also need robust orientation, allowing them to understand their role and the company's financial reporting process, so they can add value sooner.

(xi) Resources and Special Investigations

Audit committees' rights and willingness to access needed resources further support their shift to being self-sufficient and autonomous. This requires that the audit committee is ready to direct special investigations. Crises may develop suddenly and arise in unexpected places. Among the advice to committees directing a special investigation is the importance of acting quickly, ensuring the investigating firm is independent, being comfortable with the level of communication, cooperating with regulators, and ensuring appropriate remedial actions.

(p) Roles and Responsibilities of Other Committees

Other committees may include the governance committee, compensation (remuneration) committee, special committee, nominating committee, finance committee, employee benefits committee, and specific committees, such as ethics, policy, or technology committees, as needed.

The **governance committee** maximizes the effectiveness of the board through an annual review and evaluation of the structure, size, composition, development, and selection of the board members and its committees.

The **compensation committee** focuses on compensation arrangements for the board of directors and key executives that help achieve the organization's objectives and that do not emphasize short-term results at the expense of long-term performance.

It is considered good practice in an increasing number of countries that compensation (remuneration) policy and employment contracts for board members and key executives be handled

by a **special committee** of the board comprising either wholly or a majority of independent directors, There are also calls for a remuneration committee that excludes executives that serve on each others' remuneration committees, which could lead to conflicts of interest.

The **nominating committee** provides control over the selection of candidates for the board of directors and the key executives such as the CEO.

The **finance committee** controls major commitment of funds and ensures that capital expenditure budgets are consistent with strategic and operational plans.

The **employee benefits committee** oversees employee benefit programs and ensures that they are consistent with the organization's objectives and that fiduciary responsibilities are properly discharged.

(q) Various Types of Audits in Governance

In this section, various types of audits, such as stakeholder audit, governance audit, strategic audit, and due diligence audit, are briefly discussed to monitor corporate governance policies, procedures, and activities.

- **Stakeholder audit.** The stakeholder audit is a systematic and structured review of identifying issues and problems related to stakeholders (e.g., rights and privileges), and making recommendations to resolve such issues and problems.
- **Governance audit.** The corporate governance audit is a systematic and structured review of identifying issues and problems related to disclosure and transparency in the areas of financial situation, performance reporting, ownership, and board responsibilities and making recommendations to resolve such issues and problems.

  Some forward-thinking corporations in the United States have installed a CGO position or equivalent to promote good corporate governance practices. The CGO position must be a permanent one, not a one-time job created to handle a corporate crisis situation. Stakeholders will invite the permanent establishment of a CGO position since it sends a positive signal to the capital markets. This good news, in turn, increases the market price of a company's stock and lowers the cost of capital for the company. Like any other sensitive position, a corporation's internal environment, consisting of directors and management, must be supportive of good governance principles and in the hiring and functioning of a CGO job. In order to fulfill the roles and responsibilities, the CGO should have a free and full access to all board members and the chairperson of the board. To preserve his or her independence and objectivity, the CGO should report to the board, not to the CEO. Note that corporate governance practices vary greatly around the world, just as legal and ethical practices do.
- **Strategic audit.** The strategic audit is a systematic and structured review of identifying issues and problems in the understanding and execution of the approved corporate strategy in various business functions and activities and making recommendations to resolve such issues and problems. The strategic audit should focus on deciding whether a corporation is creating a value-based organization, not a profit maximization or stock price maximization organization.
- **Due diligence audit.** Due diligence audits are performed in several areas of business. They provide a safety valve to management that is: planning to acquire, manage, or consolidate

with other businesses; starting joint ventures; and environmental audits. These audits are the minimum managerial requirements to ensure that all applicable laws and regulations are met and that risks and exposures are minimized. For example, due diligence audits are risk management tools for banks, land buyers, and lending agencies when a buyer is purchasing land or accepting it as a gift. Here the buyer wants to minimize the potential legal liability resulting from the land acquisition.

Due diligence audits are team-based effort with internal auditors, EAs, lawyers, engineers, information technology (IT) staff, and other specialists. Three phases in this audit include information gathering (phase 1), information analysis (phase 2), and information reporting (phase 3). Information gathering involves collecting information through document reviews, interviews, and meetings. Information analysis may include analytical reviews, including ratio analysis, regression analysis, and other quantitative techniques. Information reporting includes writing a balanced report based on facts with an executive summary. In addition to writing reports, oral reports can be used for immediate response and clarification of issues and findings.

1.2 Business Ethics

Corporate ethics plays an important role in ensuring good corporate governance and better corporate management. Corporate ethics and corporate governance support corporate management. Ethical lapses and dilemmas are one of the root causes of many problems that corporate management faces today.

Ethics can be defined broadly as the study of what is right or good for human beings. It attempts to determine what people ought to do or what goals they should pursue. **Business ethics**, as a branch of applied ethics, is the study and determination of what is right and good in business settings. Unlike legal analyses, analyses of ethics have no central authority, such as courts or legislatures, upon which to rely; nor do they follow clear-cut, universal standards. Nonetheless, despite these inherent limitations, it is still possible to make meaningful ethical judgments.

WHAT IS THE SCOPE OF ETHICS MANAGEMENT?

The scope of ethics management includes several categories, such as societal ethics, public ethics, personal ethics, business ethics, management ethics, professional ethics, national ethics, government ethics, family ethics, environmental ethics, and individual versus group ethics.

(a) Law, Ethics, and Economics

(i) Law

Law reflects society's codified ethics and is generally regarded to be a minimum standard of behavior for individuals and organizations. It is good to respond to spirit as well as letter of law, assuming law is the floor and ethics is the ceiling on behavior, and operating above minimum required between the floor and the ceiling. Illegal acts by definition are violation of laws, rules, or regulations. They are failures to follow requirements of laws or implementing regulations, including intentional acts (e.g., fraud, irregularities, and not fully disclosing in financial statements), unintentional noncompliance acts (e.g., errors), and criminal acts. Abuse occurs when the conduct of an activity or function falls short of expectations for prudent behavior. Abuse is

distinguished from noncompliance in that abusive conditions may not directly violate laws or regulations. Abusive activities may be within the letter of the laws and regulations but violate their spirit or the more general standards of impartial behavior and, more specifically, ethical behavior. This means that abusive acts can be legal but unethical.

Some corporate executives are under the false impression that their actions are above legal and ethical principles and that they will not get caught for their bad behavior. Instead, they should realize that no one is above the law. Honesty and integrity should be the hallmark of the management profession for business managers and executives.

It is illegal for corporate management to create complicated and convoluted business divisions and ventures simply to divert the law, thus creating illusionary profits and deceiving stakeholders. The underlying, implicit intent could be to increase the company's stock price and to receive higher compensation for executives because compensation levels are tied to performance levels (i.e., profits, stock prices, and earnings per share [EPS]). If caught, these executives can be fined, punished, and imprisoned for conducting illegal activities and for their bad behavior. Human greed, at its maximum, is at play here.

(ii) Ethics

Ethics deals with deciding and acting on what is right or wrong in a particular situation. Basically, ethics is concerned with knowing what is good and bad and separating them. The following guidelines can assist business managers and executives in being ethical in a business setting.

Most ethical dilemmas involve a conflict between the needs of the part and those of the whole—the individual versus the organization or the organization versus society as a whole. Managers faced with tough ethical choices often benefit from a normative approach—one based on norms and values—to guide their decision making.

Four normative approaches are the utilitarian approach, the individualism approach, the moral-rights approach, and the justice approach. The utilitarian approach is based on the ethical concept that moral behaviors produce the greatest good for the greatest number. The individualism approach is based on the ethical concept that acts are moral when they promote the individual's best long-term interests, which ultimately leads to the greater good. The moral-rights approach is based on the ethical concept that moral decisions are those that best maintain the rights of those people affected by them. The justice approach is based on the ethical concept that moral decisions must be based on standards of equity, fairness, and impartiality.

Three types of justice are of concern to business managers: distributive, procedural, and compensatory justice. Distributive justice requires that different treatment of people not be based on arbitrary characteristics. Procedural justice emerges from the concept that rules should be clearly stated and consistently and impartially enforced. Compensatory justice requires that individuals should be compensated for the cost of their injuries by the party responsible and that individuals should not be held responsible for matters over which they have no control.

It is unethical for corporate management to create illusory profits and manipulate profits to increase their company's stock price using creative accounting practices, thus deceiving stakeholders. The underlying, implicit intent could be to increase the company's stock price and to receive higher compensation for executives because compensation levels are tied to performance

levels (i.e., profits, stock prices, and EPS). If caught, these executives can be fined, punished, and imprisoned for conducting unethical activities. Note that illegal activities and unethical activities go hand in hand sometimes but not all the times.

(iii) Law and Ethics

The generally accepted view of ethics is that ethical behavior places above behavior required by the law. Note that in many respects the law and ethics overlap because the law embodies notions of ethics. That is, the law may be seen as a reflection of what society thinks are minimal standards of conduct and behavior. Both law and ethics have to do with what is deemed appropriate or acceptable, but law reflects society's codified ethics. Therefore, if a person breaks a law or violates a regulation, he or she is also behaving unethically.

It is important to note that the law does not address all realms in which ethical questions might be raised. Thus, there are clear roles for both law and ethics to play in the society. To rephrase it, not all unethical actions are illegal (e.g., the dumpster diving act is unethical but is legal in some states) or not all illegal actions are unethical (e.g., the trespassing act is illegal but is ethical). Note that the trespassing act is involved in conducting the dumpster diving act, meaning that illegal acts are done unethically. Similarly, pirated software, movies, music, sports, and other entertainment acts are illegal and unethical in the United States but not so in most of other countries.

Note that laws and ethics relating to bribery, corruption, and violation of intellectual property rights vary greatly between the United States and other countries in that they are illegal and unethical in the United States and not so in most of other countries.

(iv) Interactions Among Law, Ethics, and Economics

Business managers and executives can use Venn diagrams to understand the interactions (i.e., connections and disconnections) among law, ethics, and economics (profits). A firm's legal, ethical, and economic goals can be depicted in a Venn diagram showing how certain decisions address these goals. Four overlapping areas and their associated scenarios are possible when these three goals are interacted (see Exhibit 1.1).

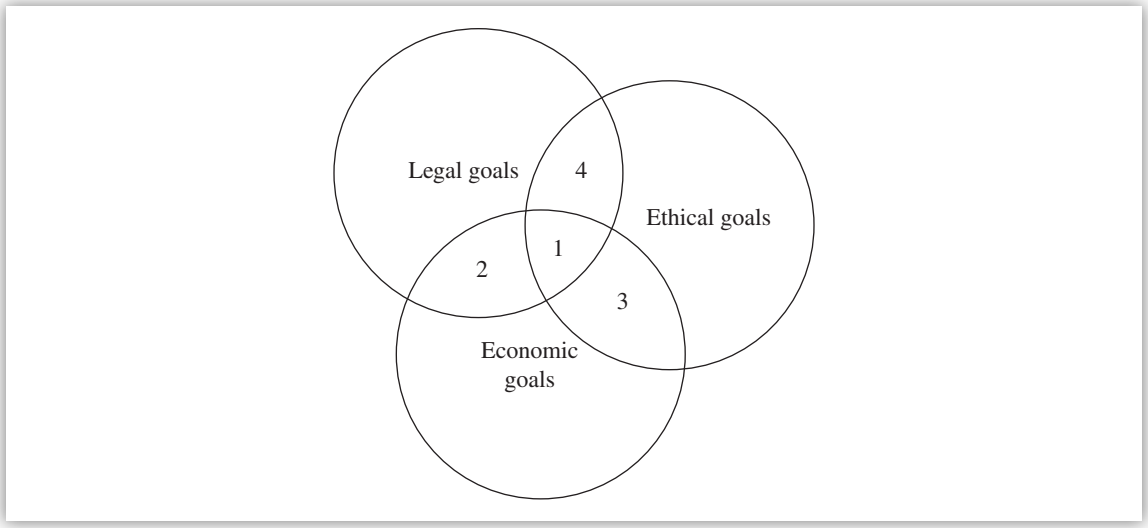


EXHIBIT 1.1 Interactions Among Law, Ethics, and Economics

Scenario 1 addresses all three goals, meaning that management's decisions are profitable, legal, and ethical. This is an ideal solution and the best situation because it meets legal, ethical, and economic goals. Here there is a connection with the law, ethics, and economics, which could be a rare situation in practice.

Scenario 2 addresses only legal and economic goals, not ethical goals. It means that management's decisions are legal and profitable but not ethical. The ethical aspect of the decision needs to be carefully considered before proceeding with this scenario. Here there is a disconnection with ethics.

HOW CAN THE VENN DIAGRAM HELPS MANAGERS?

Business managers can use Venn diagrams to understand the interactions (i.e., connections and disconnections) among law, ethics, and economics (profits). A firm's legal, ethical, and economic goals can be depicted in a Venn diagram showing how certain decisions address these goals.

Scenario 3 addresses only ethical and economic goals, not legal goals. It means that management's decisions are ethical and profitable but not legal. It could be that the law is vague or does not address the current issue. A general belief is that if something is ethical, there is a good chance it is also legal, but management cannot assume this belief and needs to proceed carefully with this scenario. Here there is a disconnection with the law.

Scenario 4 addresses only legal and ethical goals, not economic goals. It means that management's decisions are legal and ethical but not profitable. Here management has a choice of avoiding this decision altogether or finding ways to make it profitable elsewhere because this decision contradicts the profit maximization goal. However, there may be a compelling reason (e.g., government mandate to clean up pollution) to make this decision. Here there is a disconnection with economics.

(b) Basic Ethical and Legal Principles

Basic ethical and legal principles guide managers and executives to handle legal and ethical problems and issues on a day-to-day basis. When these principles are understood and implemented, they can reduce legal risks and ethical embarrassments and protect reputation in the eyes of the public.

Due process means following rules and principles so that an individual is treated fairly and uniformly at all times with basic rights protected. It also means fair and equitable treatment to all concerned parties so that no person is deprived of life, liberty, or property without due process of the law, which is the right to notice and a hearing. Due process requires due care and due diligence.

Two types of due process exist: procedural due process and substantive due process. Procedural due process ensures that a formal proceeding is carried out regularly and in accordance with established rules and principles. Substantive due process deals with a judicial requirement that enacted laws may not contain provisions that result in the unfair, arbitrary, or unreasonable treatment of an individual. It protects personal property from governmental interference or possession.

Due care means reasonable care that promotes the common good. It involves maintaining minimal and customary practices**.** Due care implies reasonable care and competence, not infallibility

or extraordinary performance. Corporate directors and officers of a corporation must perform their duties in good faith and in a nonnegligent manner. Doing this requires due care and due diligence, which are part of due process. The concepts of due care and due diligence are similar to the prudent person or reasonable person concept.

Duty of due care is the legal obligation that each person has to others not to cause any unreasonable harm or risk of harm resulting from careless acts. Negligence is a breach of the duty of due care. Corporate directors and officers must use due care and due diligence when acting on behalf of a corporation. The concepts of due care and duty of care are similar in nature.

The business judgment rule is a legal presumption that directors and officers of a corporation have exercised due care by acting on an informed basis, in good faith, and in the honest belief that their actions are in the best interests of the corporation. Unless a plaintiff can give persuasive evidence against at least one of the criteria, corporate directors and officers are insulated from liability for breach of the duty of care.

Due diligence requires organizations to develop and implement an effective system of controls, policies, and procedures to prevent and detect violation of policies and laws. In other words, due diligence is the care that a reasonable person exercises under the circumstances to avoid harm to other persons or to their property. Due diligence is another way of saying due care. Often a due diligence review is conducted when one company acquires or merges with another firm. Another related concept of due care is good faith, which means showing honesty in fact and honesty in intent. The concepts of due care and due diligence are similar to the prudent person concept.

Examples of due care and due diligence are presented next.

- Acquiring a business insurance policy is needed to protect physical assets against theft, loss, or damage.
- Training employees in information security is needed to show that a standard of due care has been taken in protecting information assets.
- Requiring acknowledgment statements that state employees have read and understood computer security requirements.
- Maintaining good housekeeping in a computer data center is needed to prevent accidents, damages, and disasters.

Gross negligence means reckless behavior with willful intent to harm people and damage property.

Due professional care applies to professionals, such as business managers and executives, accountants, auditors, engineers, lawyers, doctors, and others. Individuals should apply the care and skill expected of a reasonable prudent and competent professional during their work. Due professional care does not imply infallibility. Having proper knowledge, skills, and abilities is the major issue here. Due professional care is related to due care and due diligence.

Duty of reasonable care is the same as the duty of due care. In this regard, the business judgment rule says that directors and officers are not liable to the corporation or its shareholders for honest mistakes of judgment and for practicing the reasonable care a prudent person would do under similar circumstances.

Duty of slight care is a duty not to be grossly negligent in caring for something in one's responsibility. For example, common carriers (e.g., truckers and movers) owe this duty, which says that if the goods are lost, damaged, destroyed, or stolen, the common carrier is liable even if it was not at fault for the loss.

Duty of ordinary care is the duty an owner owes an invitee or a licensee to prevent injury or harm when the invitee or licensee steps on the owner's premises. For example, banks for proper handling of checks, individual home owners for providing safe and secure premises, and commercial and office building owners for providing safe and secure premises come under the duty of ordinary care provision.

Duty of utmost care is a duty of care that goes beyond ordinary care. It says that common carriers (e.g., airlines, buses, taxies, and coaches) and innkeepers (e.g., hotels, motels, and resorts) have a responsibility to provide security to their passengers or guests.

Duty of loyalty is expected of board of directors and officers of a corporation; they have a duty not to act adversely to the interests of the corporation and to subordinate their personal interests to those of the corporation and its shareholders. These adverse actions include self-dealing, taking personal advantage of a corporate opportunity, and competing with the corporation, thus creating conflict-of-interest situations. Under the duty of loyalty, a corporation can sue a director or an officer to recover the secret profit made on a business transaction.

WHAT ARE THE ETHICAL PRINCIPLES EXPECTED OF CORPORATE DIRECTORS AND OFFICERS?

- Due care (e.g., reasonable care, good faith, and prudent person)
- Duty of due care (e.g., no harm, nor risk, and no breach of duty)
- Due diligence (e.g., honesty in fact and honesty in intent)
- Duty of loyalty (e.g., no self-dealing, no stealing of company opportunities, no competition with the company, and no making of secret profits)

(c) Codes of Conduct

Corporate governance objectives are also formulated in voluntary codes and standards (i.e., codes of conduct) that do not have the status of law or regulation. While such codes play an important role in improving corporate governance arrangements, shareholders and other stakeholders may be uncertain concerning their status and implementation. When codes and principles are used as national standards or as explicit substitutes for legal or regulatory provisions, market credibility requires that their status in terms of coverage, implementation, compliance, and sanctions is clearly specified.

The corporation's codes of conduct document should be distributed to all employees annually. They must acknowledge receiving it, reading it, and understanding it, and must sign it stating that they employee will abide by the contents of the document.

World-class organizations have developed codes of conduct for their organizations, which should comply with the definition of a "code of ethics" set out in Section 406 (c) of the Sarbanes-Oxley (SOX) Act of 2002. In addition, the code must provide for an enforcement mechanism

and protection for persons reporting questionable behavior (i.e., whistleblowing). The board of directors must approve any waivers of the code for directors, executives, or officers of the organization.

(d) Financial Disclosures

In the U.S. federal government, the Ethics in Government Act of 1978 requires financial disclosure reporting, The reporting is intended to identify and deter conflicts of interest between the duties and responsibilities of federal employees and their personal financial interests and activities. Depending on such matters as the position held or the amount of compensation, disclosure statements are either to be made available to the public or kept confidential by the agencies.

Similarly, executives, board of directors, consultants, and contractors working for a private company are required to submit financial information regarding stocks and bonds that they hold in the company. They also must disclose any other conflict-of-interest situations that can impair their independence and objectivity.

(e) U.S. Foreign Corrupt Practices Act

In 1977, the U.S. Congress enacted the Foreign Corrupt Practices Act (FCPA) prohibiting all U.S domestic concerns from bribing foreign governmental or political officials. In addition to antibribery provisions, the FCPA contains provisions pertaining to accounting and internal control. These provisions require corporate management to maintain books, records, and accounts that accurately and fairly reflect the transactions and dispositions of the corporation's assets and to devise and maintain a system of internal accounting control adequate to accomplish certain financial objectives. Thus, a key theme underlying the FCPA was that sound internal control should provide an effective deterrent to illegal payments.

In 1998, the U.S. Congress enacted the International Anti-Bribery and Fair Competition Act to conform the FCPA to the OECD Convention. In essence, the 1998 Act expands the scope of the FCPA.

In FCPA, bribery and corruption payments are classified into three major types. Grease payments (petty payments) are made to nonelected public officials. Grand payments are made to elected, higher-ranked public or political officials. Influence peddling payments involve political campaign contributions. Note that the FCPA allows grease payments for competitive advantage; the other types of payments are not allowed.

(f) U.S. Federal Securities Regulations

The primary purpose of U.S. federal securities regulations is to prevent fraudulent practices in the sale of investment securities and thereby to foster public confidence in the securities market. Two federal statutes include the Securities Act of 1933, which focuses on the issuance of original securities (primary market transactions), and the Securities Exchange Act of 1934, which deals mainly with trading in issued securities (secondary market transactions). These secondary market transactions greatly exceed in volume and value the original offerings by issuers. The Securities and Exchange Commission (SEC) administers both of these securities acts. The 1933 Act mainly focuses on information provided to investors to prohibit misrepresentation and deceit. The 1934

Act primarily focuses on disclosure requirements and regulates tender offers and proxy solicitations. Foreign issuers who issue securities or whose securities are sold in the secondary market in the United States must register them in the United States with the SEC unless an exemption is available (www.sec.gov).

(g) U.S. Sarbanes-Oxley Act of 2002

Responding to corporate failures and fraud that resulted in substantial financial losses to institutional and individual investors, the U.S. Congress passed SOX in 2002. As shown next, the act contains provisions affecting the corporate governance, auditing, and financial reporting of public companies, including provisions intended to deter and punish corporate accounting fraud and corruption. SOX generally applies to those public companies required to file reports with SEC under the Securities Exchange Act of 1933 and the Securities Exchange Act of 1934 and to registered accounting firms (www.pcaobus.org).

Section 101: Public Company Accounting Oversight Board Establishment. Establishes Public Company Accounting Oversight Board (PCAOB) to oversee the audit of public companies that are subject to the securities laws.

Section 102: Registration with the PCAOB. This section requires accounting firms that prepare or issue audit reports to public companies to register with PCAOB.

Section 103: Auditing, Quality Control, and Independence Standards and Rules. This section requires PCAOB, by rule, to establish auditing and other professional standards to be used by registered public accounting firms in the preparation and issuance of audit reports.

Section 104: Inspections of Registered Public Accounting Firms. This section requires PCAOB to annually inspect registered public accounting firms with more than 100 issuer audit clients and triennially inspect registered public accounting firms with 100 or less issuer audit clients.

Section 105: Investigations and Disciplinary Proceedings. This section requires PCAOB to establish fair procedures for investigating and disciplining registered public accounting firms and associated persons and authorizes PCAOB to investigate and discipline such firms and persons.

Section 201: Services Outside the Scope of Practice of Auditors. Registered accounting firms cannot provide certain nonaudit services to a public company if the firm also serves as the auditor of the financial statements for the public company. Examples of prohibited nonaudit services include bookkeeping, appraisal or valuation services, internal audit outsourcing services, and management functions.

Section 301: Public Company Audit Committees. Listed company audit committees are responsible for the appointment, compensation, and oversight of the registered accounting firm, including the resolution of disagreements between the registered accounting firm and company management regarding financial reporting. Audit committee members must be independent.

Section 302: Corporate Responsibility for Financial Reports. For each annual and quarterly report filed with SEC, the CEO and CFO must certify that they have reviewed the report and, based on their knowledge, the report does not contain untrue statements

or omissions of material facts resulting in a misleading report and that, based on their knowledge, the financial information in the report is fairly presented.

Section 304: Forfeiture of Certain Bonuses and Profits. The CEO and CFO of the issuer have to reimburse the issuer for any bonus or profits from sale of securities during the 12-month period following the filing of a financial document that required an issuer to prepare an accounting restatement due to misconduct.

Section 308: Fair Funds for Investors. Civil penalties can be added to the disgorgement fund for the benefit of the victims of a security law violation. A disgorgement sanction requires the return of illegal profits.

Section 404: Management Assessment of Internal Controls. This section consists of two parts. First, in each annual report filed with SEC, company management must state its responsibility for establishing and maintaining an internal control structure and procedures for financial reporting; it must also assess the effectiveness of its internal control structure and procedures for financial reporting. Second, the registered accounting firm must attest to, and report on, management's assessment of the effectiveness of its internal control over financial reporting.

Section 406(c): Code of Ethics. This section must provide for an enforcement mechanism and protection for persons reporting questionable behavior (i.e., whistleblowing). The board of directors must approve any waivers of the code for directors, executives, or officers of the organization.

Section 407: Disclosure of Audit Committee Financial Expert. Public companies must disclose in periodic reports to SEC whether the audit committee includes at least one member who is a financial expert and, if not, the reasons why.

(h) Key Ethical Principles

Examples of key ethical principles are listed next.

- **Golden Rule.** One should put oneself in others' shoes. It includes not knowingly doing harm to others.
- **Means-ends cycle.** When ends are of overriding importance, unscrupulous means may be used to reach the ends.
- **Might-equals-right principle.** Justice is defined as the interest of the stronger, meaning that stronger people have an upper hand over the weaker people.
- **Professional principle.** A true professional will do things in such a way that he or she can explain them before a committee of peer professionals.
- **Goal congruence principle.** Actions, wills, and needs of employees should be subordinated to the greater good of the organization they work for. Employees should ask themselves whether their goals are consistent with the organization's goals. This principle is similar to the utilitarian ethic, meaning the greatest good should be done for the greatest number, and to the organization ethic, meaning that employees do things for the good of the organization.
- **Prudent person concept.** The prudent person, who is not infallible or perfect, has the ability to govern and discipline him- or herself by the use of reason; does not neglect duty; and applies knowledge, skills, and sound judgment in the use of organization's resources. The prudent person concept is related to the goal congruence principle.

(I) Ethical Dilemmas

Managers and executives in both the private and the public sector often face ethical dilemmas during their job duties. Some examples of these ethical dilemmas that may help to clarify the definition of business or government ethics are discussed next.

- In the interaction between a pharmaceutical company and a medical researcher, the company management threatens the researcher if he releases negative test results (bad news) to the public about its drugs.
- In the interaction between government attorneys and a government executive, attorneys are fired improperly for whistleblowing on the government and not following the executive's unethical instructions despite the Ethics in Government Act and the Whistleblower Protection Act.
- In the interaction between a local oil company and local government officials, the oil company was allowed to dump toxic substances into a nearby lake, which is used for drinking water, in exchange for creating more local jobs when the oil company expands its plant processing capacity. The toxic substances kill fish and grow seaweed in the lake and cause algae blooms.
- In the interaction between federal environmental regulators and management of a very old coal-fired power plant, regulators relaxed rules to allow the reopening of the plant after it was closed due to the excessive air pollution it generated. The plant required modernization work to reduce air pollution, and the work was not completed when the plant was reopened.
- In the relationships between employees and employers, many issues arise regarding the safety and compensation of workers, their civil rights (such as equal treatment, privacy, and freedom from sexual harassment), and the legitimacy of whistleblowing. Tax and legal issues can arise when previous employees work as contractors.
- In the relationships between business and its customers, ethical issues permeate marketing techniques, product safety, price discrimination, and consumer protection.
- In the relationships between business and its owners, ethical questions involving corporate governance, shareholder voting, and management's duties to the shareholders can pose problems.
- Relationships among competing businesses involve numerous ethical matters, including fair competition and the effects of collusion in price fixing and other matters.
- In the relationships between buyers and vendors, suppliers, contractors, and consultants, showing favors and receiving bribes and expensive gifts are common.
- In the interaction between gatekeepers (e.g., external auditors (EAs), attorneys, securities analysts [SAs], and investment bankers [IBs]) and their owners, gatekeepers do not always discharge their professional responsibilities in the financial securities and capital markets due to conflicts of interest, job security, groupthink (e.g., consensus earnings forecasts with peers), and greed.
- The interaction between business and society at large presents additional ethical dimensions, such as pollution of the physical environment, commitment to the community's economic and social infrastructure, and depletion of natural resources.
- At the international level, issues such as bribery of foreign officials, exploitation of less-developed countries, and conflicts among differing cultures and value systems are difficult to control and monitor.

- In the interaction between a company management and investors and the stock market, company management can manipulate earnings and profits (earnings management) to boost its stock prices and to receive big bonuses when the actual financial results are less than expected.
- In the interaction between a company management and the bond market and the stock market, company management can hide its debt through off–balance sheet accounting practices to realize higher bond prices and higher stock prices. This practice is unethical although not illegal because GAAP allows it.
- In the interaction between a company management and the board of directors, company management can pull off financial shenanigans (a form of financial fraud) against the company. The board of directors may not be able to prevent and detect such acts, but it is legally liable for such unethical conduct on part of company management.
- In the interaction between buyers and sellers of a company, both parties might employ unethical and illegal tactics to win or lose the mergers and acquisitions.

(j) Transparency International's Corruption Perceptions Index

Transparency International is the world's foremost anticorruption lobbying organization. It measures the perceived levels of public sector corruption in 183 countries and territories around the world. It develops and publishes a corruption perceptions index. The 2011 index showed that public frustration is well founded. No region or country in the world is immune to the damages of corruption, and the vast majority of the 183 countries and territories assessed score below 5 on scale of 0 (highly corrupt) to 10 (very clean). New Zealand, Denmark, Finland, and Canada top the list (very clean), while North Korea and Somalia are at the bottom (highly corrupt). Note that these indexes may change over time (visit www.cpi.transparency.org/ cpi2011/).

(k) Types of Ethics

Basically, ethics can be of two types: normative and descriptive. Managers faced with tough ethical choices often benefit from a **normative approach**—one based on norms and values—to guide their decision making. Normative ethics is concerned with supplying and justifying a coherent moral system of thinking and judging. It asks: What ought to be? Normative approach includes utilitarian, individualism, moral rights, and justice approaches. An application of the normative approach can occur when a decision is made to recruit, hire, train, and promote men and women equally.

The **descriptive ethics approach** is concerned with describing, characterizing, and studying the morality of a people, a culture, or a society. It also compares and contrasts different moral codes, systems, practices, beliefs, and values. It asks a basic question: What is? The business judgment rule is a legal presumption that the directors and officers of the corporation have exercised due care by acting on an informed basis, in good faith, and in the honest belief that their actions are in the best interests of the corporation. Unless a plaintiff can give persuasive evidence against at least one of the criteria, corporate directors and officers are insulated from liability for breach of the duty of care. A downside is that some people may adopt the view that "if everyone is doing it, it must be acceptable," which is not right. Examples include discrimination, speeding while driving a car, padding expense accounts, and deceptive advertising.

NORMATIVE APPROACH VERSUS DESCRIPTIVE APPROACH

- The normative approach deals with what ought to be or what ought not to be in the prevailing set of ethical standards.
- The descriptive approach focuses on what is in the prevailing set of ethical standards.

One should compare what ought to be with what is to see what is going on in the real world.

Three major approaches to thinking about business ethics include the conventional approach, the principles approach, and the ethical tests approach. In the **conventional approach** to business ethics, we compare a decision or practice with prevailing norms of acceptability. It is called the conventional approach because it is believed that this is the way that general society thinks.

The **principles approach** includes the utilitarian ethic, virtue ethic, and the Golden Rule, and augments the conventional approach to business ethics. The utilitarian ethic focuses on providing the greatest good for the greatest number. The Golden Rule includes not knowingly doing harm to others.

The **ethical tests approach** is based on practice while the principles approach is based on philosophy (e.g., servant leadership). Showing common sense, presenting one's best self, making something public, and ventilation are examples of the ethical test approach.

(I) Models of Management Ethics

The three models of management ethics include immoral management, moral management, and amoral management.

The **immoral management** model holds that management's motives are selfish and greedy and that management cares only about its own or its company's gains. For example, if Company A knowingly commits a wrongful act that is detrimental to Company B, Company A has exhibited an immoral type of management ethics. Immoral management decisions, behaviors, actions, and practices are discordant with ethical principles. They represent unethical behavior and follow an exploitive strategy.

Moral management, as expected, exhibits ethical behavior and follows the integrity strategy. It conforms to the highest standards of ethical behavior or professional standards of conduct.

Amoral management can be intentionally or unintentionally amoral. Intentionally amoral managers do not factor ethical considerations into their decisions, actions, and behaviors because they believe business activity resides outside the sphere to which moral judgments apply. They think that different rules apply in business than in other areas of life. Unintentionally amoral managers do not think about business activity in ethical terms. These managers are simply casual about the negative effects of their decisions on others. They lack ethical perception and moral awareness and do not stop to consider that their actions have ethical dimensions or consequences. Amoral management contains both intentional and unintentional behavior and follows compliance strategy.

(m) Elements of Making Moral Judgments

The six major elements or capacities that are essential to making moral judgments include:

1. Moral imagination.
2. Moral identification and ordering.
3. Moral evaluation.
4. Tolerance of moral disagreement and ambiguity.
5. Integration of managerial and moral competence.
6. A sense of moral obligation and integrity.

Moral imagination refers to the ability to perceive that a web of competing economic relationships is, at the same time, a web of moral or ethical relationships. Developing moral imagination means not only becoming sensitive to ethical issues in business decision making but also developing the perspective of searching out subtle places where people are likely to be detrimentally affected by decision making or behaviors of managers.

Moral identification and ordering refers to the ability to discern the relevance or nonrelevance of moral factors that are introduced into a decision-making situation. The goal of **moral evaluation** is to integrate the concern for others into organizational goals, purposes, and legitimacy. In the final analysis, though, the manager may not know the "right" answer or solution, although moral sensitivity has been introduced into the process. The important point is that amorality has not prevailed or driven the decision process.

Tolerance of moral disagreement and ambiguity is an extension of a managerial talent or facility that is present in all decision-making situations managers face. **Integration of management and moral competence** combines management's knowledge, skills, and abilities with moral values that provide future-looking perspective**. A sense of moral obligation and integrity** requires the intuitive or learned understanding that moral fibers—a concern for fairness, justice, and due process to people, groups, and communities—are woven into the fabric of managerial decision making and are integral components that hold systems together.

(n) Roles and Responsibilities of Gatekeepers

Gatekeepers include EAs, attorneys, SAs, CRAs, and IBS, who inform and advise the board of directors and the shareholders, are not fulfilling their gatekeeper or agent role to its fullest extent. These gatekeepers should be serving investors, creditors, and stockholders by assuming an independent monitor or watchdog role and by avoiding conflict-of-interest situations that can compromise their independence and objectivity.[6]

Gatekeepers are in a way police officers to prevent corporate wrongdoings. Some examples of corporate wrongdoing include manipulating earnings (earnings management), financial restatements, capitalizing expenses, deferring or misclassifying expenses, hiding liabilities, engaging in off–balance sheet transactions, and involving in other types of financial fraud to increase stock price and to receive big bonuses.

[6] John C. Coffee Jr., *Gatekeepers: The Professions and Corporate Governance* (New York: Oxford University Press, 2006).

Gatekeepers provide certification and verification services to investors. They are hired and paid by the corporate managers that they are to watch. The impact of these services is to lower the cost of capital for a corporation and thereby increase its stock price. Both shareholders and the board of directors depend on gatekeepers for an unbiased flow of information that is not edited, filtered, or modified in favor of corporate management. Effective corporate governance requires a chain of actors including directors, managers, and gatekeepers, where the latter cannot become the weakest link. Taken to the extreme, the board of directors and the SEC can also be viewed as gatekeepers.

Gatekeepers are not fulfilling their watchdog role in preventing and/or detecting fraud or other irregularities. Gatekeepers should not wear blinders, cannot ignore red flags, cannot be indifferent to sins of omissions, and cannot do perfunctory audits or investigations.

Gatekeepers should increase their positive reputational capital and decrease their negative reputational capital by exhibiting unbiased and professional behavior.

Organizations should do the following to control gatekeepers:

- The board of directors should be active and independent of corporate management to discharge their fiduciary responsibilities. The board should not approve loans to the CEO or other executives.
- A principal–agent relationship between gatekeepers and the corporation must be reconsidered and restructured.

Organizations should *not* do opinion shopping for accounting, auditing, and legal services.

(i) Role of External Auditors as Gatekeepers

The roles and responsibilities of EAs as gatekeepers are listed next.

- EAs certify that a corporation's financial statements comply with GAAP, which are too soft and permissive.
- EAs are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.
- EAs who discover a serious problem with a corporate client's financial statements or disclosures can prevent a merger from closing by declining to deliver an opinion that is a necessary precondition for that transaction.
- EAs should be faithful to investors and should not provide false or reckless certification. They should not ignore red flags.
- EAs should use professional skepticism when dealing with corporate management assertions.
- EAs should act like gatekeepers, not like salespersons.

(ii) Role of Attorneys as Gatekeepers

The roles and responsibilities of attorneys as gatekeepers are listed next.

- Attorneys should conduct due diligence reviews in connection with an organization's securities offerings.

- Attorneys are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.
- Attorneys who discover a serious problem with a corporate client's financial statements or disclosures can prevent a merger from closing by declining to deliver an opinion that is a necessary precondition for that transaction.
- Attorneys should use professional skepticism when dealing with corporate management representations.
- Attorneys should comply with Section 307 of SOX , which prescribes minimum standards of professional conduct for attorneys who appear or practice before the SEC. This section requires an up-the-ladder reporting obligation; in other words, a material violation should be reported to the audit committee or the full board of directors only after the attorney did not receive an appropriate response within a reasonable time after reporting a violation to the chief legal officer or the CEO.

(iii) Role of Securities Analysts as Gatekeepers

The roles and responsibilities of SAs as gatekeepers are listed next.

- SAs' positive evaluation may lend credibility to a company's own disclosures or predictions.
- SAs test and interpret financial statements and corporate disclosures. Based on this information, they make their own extrapolations and predictions as to the corporation's future financial and operational performance. They then issue research reports after meeting with company management and discussing with industry sources, such as customers and suppliers.
- SAs issue buy, hold, or sell recommendations to their customers and the public. These recommendations are often inconsistent with a company's actual performance levels due to fear of retaliation, job security (career prospects), groupthink, income potential, and conflict-of-interest situations.
- SAs should not make excessively optimistic financial forecasts about a company by overstating future earnings and inflating recommendations.
- SAs should act like gatekeepers, not like salespersons.

(iv) Role of Credit Rating Agencies as Gatekeepers

The roles and responsibilities of CRAs are listed next.

- CRAs (e.g., Moody's and Standard &Poor's) provide a standardized and condensed information about the creditworthiness of bonds of a corporation.
- CRAs assign a letter rating, ranging from AAA to D, to a corporation's debt securities. The debt rating influences the cost of capital of the debt-issuing firm.
- CRAs are hesitant to downgrade a company's rating due to bankruptcy that it can trigger in the marketplace. CRAs should lead, not follow, the market.
- CRAs are paid by the companies that they rate and do not face severe competition in the marketplace.
- CRAs should not accept consulting services from the issuers that they rate.

(v) Role of Investment Bankers as Gatekeepers

The roles and responsibilities of IBs are listed next.

- IBs deliver a fairness opinion in a cash-out merger that assures a company's minority shareholders that they have received a fair price.
- IBs must conduct a reasonable investigation of the statements made by the issuer in its registration statement when the issuer registers securities for public sale. This is called due diligence review. They should not solely depend on the audited financial statements and the comfort letter from the EAs.
- IBs should refuse to underwrite an issuer's securities if they find that the issuer's disclosures are materially deficient.
- IBs are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.

(o) Roles and Responsibilities of the Chief Ethics Officer

The chief ethics officer should develop an ethics manual describing policies and procedures of expected behavior of employees and other stakeholders. The content of this manual should include:

- Conflicts of interest and codes of conduct.
- Restrictions regarding accepting or giving gifts and travel by procurement, contracting, marketing, and sales personnel.
- Requiring written disclosures on executives' financial condition and outside earned income activities.
- Employing relatives and friends (nepotism or cronyism).
- Protecting an organization's property and information.
- Describing allowed political contributions and activities.
- Treatment of sale of stock acquired pursuant to exercise of stock options to comply with conflict-of-interest requirements and restrictions on sharing or using insider information.
- Protecting whistleblowing employees.

The chief ethics officer is a key person in the C-level executive suite with these roles and responsibilities:

- Promote a positive ethical climate in the organization through his or her leadership skills.
- Develop an ethics manual describing company policy, codes of conduct, and expected behavior; reporting of ethical violations; and referencing all applicable laws and regulations.
- Require each and every employee in the organization annually to sign a corporate ethics document acknowledging its receipt and that the employee has read the document and understands it, and will abide with the contents of the document.
- Conduct training classes to managers and nonmanagers about ethical principles that include actions and consequences.

- Work with the internal audit department in developing audit plans and identifying areas of audit addressing ethical violations.
- Work with the legal department in pursuing cases that violate ethical principles either inside the company (e.g., employees and management) or outside (e.g., customers, suppliers, vendors, and contractors).
- Conduct ethics audits, special management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in ethical matters.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnects between these views and to integrate them in a coherent manner.

(p) Roles and Responsibilities of the Chief Legal Officer

The corporate chief legal officer (or corporate legal counsel or corporate general counsel):

- Establishes policies and procedures relating to prosecution of identified instances of fraud, waste, and abuse cases and employee criminal acts.
- Oversees the implementation of ethics program throughout the organization.
- Handles patent, trademark, and copyright violations by individuals or organizations.
- Reviews discrimination suits filed by employees, contractors, and consultants against the corporation.
- Involves in labor union negotiations.

There is always an interaction between the chief ethics officer and the chief legal officer because some corporate issues overlap between ethics and law, and sometimes the demarcation is not clear.

Specific roles and responsibilities of the chief legal officer are listed next.

- Participate in the due diligence process during proposed mergers or acquisitions as part of subject matter experts from operations, finance, IT, and marketing.
- Develop business contracts and provide technical support to management to enforce contractual terms and conditions.
- Work with IBs and brokers in developing prospectus documents and filing securities regulation applications during stock and bond offerings to potential investors.
- Participate in labor union negotiations for a win-win outcome.
- Conduct in-house training classes for functional managers and executives regarding interpretation of laws, regulations, the Uniform Commercial Code, and court cases.
- Establish a solid and sustainable chain of knowledge linked through the entire legal management hierarchy to ensure core knowledge competencies.
- Conduct legal audits, management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in legal matters.
- Comply with professional standards and code of ethics established by the American Bar Association for the legal profession.

- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnects between these views and to integrate them in a coherent manner.

(q) Conduct an Ethics Audit

Specifically, the chief ethics officer or his or her designee should perform an ethics audit: In performing such an audit, the chief ethics officer:

- Works with the internal audit department in developing audit plans and to identify areas of audit addressing ethical violations.
- Works with the legal department in pursuing cases that violated ethical principles either inside the company (e.g., employees and management) or outside (e.g., customers, suppliers, vendors, and contractors).
- Conducts ethics audits, special management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in ethical matters.
- Encourages employees and others to report ethical violations through a whistleblower telephone hotline, e-mail, or other means that will be kept confidential.
- Conducts training classes for managers and nonmanagers about ethical principles that include actions and consequences and referencing to all the applicable laws and regulations.
- Analyzes outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnects between these views and to integrate them in a coherent manner.
- Issues an audit report describing significant findings and recommendations to management for corrective actions to take.

1.3 Corporate Social Responsibility

Corporations have obligations to be good citizens of the local, national, and international communities in which they do business. Failure to meet these obligations can result in damage to the cooperation, both in immediate economic terms and in longer-term reputational value.

(a) What Is a Corporate Social Responsibility?

A corporation should be a good citizen and contribute to the communities in which it operates by making charitable contributions and encouraging its directors, managers, and employees to form relationships with those communities. A corporation also should be active in promoting awareness of health, safety, and environmental issues, including any issues that relate to the specific types of business in which the corporation is engaged. Organizations must comply with the ISO 26000 standard regarding social responsibility.

According to Carroll, the social responsibility of business encompasses the economic, legal, ethical, and discretionary (philanthropic) expectations that society has of organizations at a given point in time.[7]

[7] Archie B. Carroll, "The Four Faces of Corporate Citizenship," *Business and Society Review* 100, no. 1 (1998): 1–7.

Carroll's four-part definition attempts to place economic and legal expectations of business in context by relating them to more socially oriented concerns. These social concerns include ethical responsibilities and philanthropic (voluntary/discretionary) responsibilities. This definition, which includes four kinds of responsibilities, elaborates and builds on the definition proposed by McGuire.

(i) Economic Responsibilities

In regard to social responsibility, first there are the economic responsibilities of business. It may seem odd to call an economic responsibility a social responsibility, but, in effect, this is what it is. First and foremost, the American social system calls for business to be an economic institution. That is, it should be an institution whose orientation is to produce goods and services that society wants and to sell them at fair prices—prices that society thinks represent the true values of the goods and services delivered and that provide business with profits adequate to ensure its perpetuation and growth and to reward its investors. While thinking about its economic responsibilities, business employs many management concepts that are directed toward financial effectiveness—attention to revenues, costs, strategic decision making, and the host of business concepts focused on maximizing the organization's long-term financial performance.

SUMMARY OF ECONOMIC RESPONSIBILITIES

Society requires **economic responsibility** of business, which includes things such as being profitable, maximizing sales, minimizing costs, making sound strategic decisions, and being attentive to dividend policy.

(ii) Legal Responsibilities

Next there are legal responsibilities of business**.** Just as society has sanctioned our economic system by permitting business to assume the productive role mentioned earlier, as a partial fulfillment of the social contract, it has also laid down the ground rules—the laws—under which business is expected to operate. Legal responsibilities reflect society's view of codified ethics in the sense that they embody basic notions of fair practices as established by our lawmakers. It is business's responsibility to society to comply with these laws. If business does not agree with laws that have been passed or are about to be passed, our society has provided a mechanism by which dissenters can be heard through the political process. In the past 30 years, our society has witnessed a proliferation of laws and regulations striving to control business behavior.

As important as legal responsibilities are, these responsibilities do not cover the full range of behaviors expected of business by society. The law is inadequate for at least three reasons.

1. The law cannot possibly address all the topics, areas, or issues that business may face. New topics continually emerge, such as Internet-based business (e-commerce) and genetically engineered foods.
2. The law often lags behind more recent concepts of what is considered appropriate behavior. For example, as technology permits more exact measurements of environmental contamination, laws based on measures made by obsolete equipment become outdated but are not changed often.

3. Laws are made by lawmakers and may reflect the personal interests and political motivations of legislators rather than appropriate ethical justifications. A wise sage once said: "Never go to see how sausages or laws are made." It may not be a pretty picture.

SUMMARY OF LEGAL RESPONSIBILITIES

Society requires **legal responsibility** of business, which includes things such as obeying all laws and adhering to all regulations, obeying the Foreign Corrupt Practices Act, fulfilling all contractual obligations, and honoring warranties and guarantees.

(ii) Ethical Responsibilities

Because laws are important but not adequate, ethical responsibilities embrace those activities and practices that are expected or prohibited by societal members, even though they are not codified into law. Ethical responsibilities embody the full scope of norms, standards, and expectations that reflect a belief of what consumers, employees, shareholders, and the community regard as fair, just, and in keeping with the respect for or protection of stakeholders' moral rights.

In one sense, changes in ethics or values precede the establishment of laws because they become the driving forces behind the initial creation of laws and regulations. For example, the civil rights, environmental, and consumer movements reflected basic alterations in societal values and thus may be seen as ethical bellwethers foreshadowing and leading to later legislation. In another sense, ethical responsibilities may be seen as embracing and reflecting newly emerging values and norms that society expects business to meet, even though they may reflect a higher standard of performance than that which currently is required by law. Ethical responsibilities in this sense are often ill defined or continually under public scrutiny and open to debate as to their legitimacy. Thus, frequently they are difficult for business to agree on. Regardless, business is expected to be responsive to newly emerging concepts of what constitutes ethical practices.

Superimposed on these ethical expectations emanating from societal and stakeholder groups are the implied levels of ethical performance suggested by a consideration of the great ethical principles of moral philosophy, such as justice, rights, and utilitarianism.

We can consider ethical responsibilities as encompassing those areas in which society expects certain levels of moral or principled performance but for which it has not yet articulated or codified laws.

SUMMARY OF ETHICAL RESPONSIBILITIES

Society expects **ethical responsibility** of business, which includes things such as avoiding questionable practices; responding to the spirit as well as the letter of law; assuming law is a floor on behavior; operating above the minimum required; doing what is right, fair, and just; and asserting ethical leadership.

(iv) Philanthropic Responsibilities

Finally there are business's voluntary/discretionary or philanthropic responsibilities**.** These are viewed as responsibilities because they reflect current expectations of business by the public. These activities are voluntary, guided only by business's desire to engage in social activities that

are not mandated, not required by law, and not generally expected of business in an ethical sense. Nevertheless, the public has an expectation that business will engage in philanthropy; thus, this category has become a part of the social contract between business and society. Such activities might include corporate giving, product and service donations, volunteerism, partnerships with local government and other organizations, and any other kind of voluntary involvement of the organization and its employees with the community or other stakeholders.

WHAT IS A SOCIAL AUDIT?

A social audit is a systematic analysis and testing of an organization's success in achieving its social responsibility. It is a systematic attempt to identify, measure, monitor, and evaluate an organization's performance with respect to its social efforts, goals, and programs. The social audit is a systematic and structured review of identifying issues and problems in the understanding and fulfilling of economic, legal, ethical, and philanthropic responsibilities, and making recommendations to resolve such issues and problems.

The distinction between ethical responsibilities and philanthropic responsibilities is that the latter typically are not expected in a moral or an ethical sense. Communities desire and expect business to contribute its money, facilities, and employee time to humanitarian programs or purposes, but they do not regard firms as unethical if they do not provide these services at the desired levels. Therefore, these responsibilities are more discretionary, or voluntary, on the part of business, although the societal expectation that they be provided is always present. This category of responsibilities is often referred to as good corporate citizenship.

In essence, then, our definition forms a four-part conceptualization of corporate social responsibility (CSR) that encompasses the economic, legal, ethical, and philanthropic expectations placed on organizations by society at a given point in time. The implication is that business has accountability for these areas of responsibility and performance. This four-part definition provides categories within which to place the various expectations that society has of business. Each category is considered an indispensable facets of the total social responsibility of business. This conceptual model completely describes the kinds of expectations that society expects of business. One advantage of this model is that it can accommodate those who have argued against CSR by characterizing an economic emphasis as separate from a social emphasis. This model includes both emphases along with others that collectively make up CSR.

SUMMARY OF PHILANTHROPIC RESPONSIBILITIES

The **philanthropic responsibility** is desired of business by society, and includes things such as being a good corporate citizen, making corporate contributions, providing programs supporting the community (e.g., education, health and human services, culture, arts, and civic duties), and voluntarily providing for community development and betterment.

(b) Pyramid of Corporate Social Responsibility

A helpful way of graphically depicting the four-part definition is envisioning a pyramid composed of four layers. The pyramid portrays the four components of CSR, beginning with the basic building block of economic performance (making a profit), at the base. At the same time, business is expected to obey the law, because the law is society's codification of acceptable and

unacceptable behavior. Next is business's responsibility to be ethical. At its most basic level, this is the obligation to do what is right, just, and fair and to avoid or minimize harm to stakeholders (employees, consumers, the environment, and others). Finally, business is expected to be a good corporate citizen—to fulfill its voluntary or discretionary or philanthropic responsibility to contribute financial and human resources to the community and to improve the quality of life.

LAYERS OF CORPORATE SOCIAL RESPONSIBILITY

A socially responsible firm should strive to:

- Be a good corporate citizen (top).
- Be ethical.
- Obey the law.
- Make a profit (base).

The most critical tensions, of course, are those between economic and legal, economic and ethical, and economic and philanthropic responsibilities. The traditionalist might see this as a conflict between a firm's concern for profits and its concern for society, but we suggest that this is an oversimplification. A CSR or stakeholder perspective recognizes these tensions as organizational realities but focusses on the total pyramid as a unified whole and on how the firm might engage in decisions, actions, policies, and practices that simultaneously fulfill all component parts of the pyramid. This pyramid should not be interpreted to mean that business is expected to fulfill its social responsibilities in some sequential fashion, starting at the base. Rather, business is expected to fulfill all its responsibilities simultaneously.

In summary, the total social responsibility of business entails the concurrent fulfillment of the firm's economic, legal, ethical, and philanthropic responsibilities. In equation form, this might be expressed as:

$$\text{Total CSR} = \text{Economic responsibilities} + \text{Legal responsibilities} + \text{Ethical responsibilities} + \text{Philanthropic responsibilities}$$

1.4 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Which of the following establishes a corporation's governance mechanism?

a. Stockholders

b. Corporate bylaws

c. Board of directors

d. Corporate officers

2. A corporation must be managed on which of the following principles?

a. Corporate governance

b. Corporate control

c. Corporate law

d. Corporate ethics

3. The **major** issue embedded in the structure of modern corporations that has contributed to the corporate governance problem has been:

a. Separation of purchase from lease.

b. Separation of suppliers from producers.

c. Separation of ownership from control.

d. Separation of employees from independent contractors.

4. Which of the following is the **major** reason for agency problems to exist?

a. Owner interest

b. Self-interest

c. Community interest

d. Corporate interest

5. The practice of obtaining critical information from a company in faith and then using that information for one's own personal financial gain is called:

a. Financial trading.

b. Insider trading.

c. Shareholder trading.

d. Investor trading.

6. Which of the following is **not** an example of ethical dilemma facing a business manager involving a conflict between the:

a. Part versus whole.

b. Individual versus organization.

c. Organization versus society.

d. Individual versus family.

7. Abusive acts can be:

a. Legal but unethical.

b. Ethical but illegal.

c. Legal and ethical.

d. Illegal and unethical.

8. Which of the following statement is **not** true about ethics and law?

a. Ethical behavior resides above the legal behavior.

b. Law embodies notions of ethics.

c. Law addresses all ethical questions.

d. Law and ethics have clear roles to play in the society.

9. Which type of social responsibility embraces those activities and practices that are expected or prohibited by societal members even though they are **not** codified into law?

a. Ethical responsibilities.

b. Legal responsibilities.

c. Philanthropic responsibilities.

d. Economic responsibilities.

10. Which of the following refers to the corporate behavior in response to market forces or legal constraints?

a. Social obligation

b. Social responsibility

c. Social responsiveness

d. Social attitude

DOMAIN 2

Risk Management (10–20%)

2.1 Corporate Risk Management

Risk is pervasive throughout an organization as it can arise from any business function or process at any time without warning. Because of this widespread exposure, no single functional department management, other than the board of directors, can oversee the enterprise-wide risk management program. This approach also supports the idea that risks cannot be identified, measured, and monitored on a piecemeal basis. A holistic approach is needed.

Since risks can arise in any business function or process, it makes good sense for business unit line management to accept full responsibility for risk management with support from a centralized risk management function. The business unit line management must see that managing risk is an integral part of its mission, for example, manufacturing a product or delivering a service, where risks are linked to business objectives and strategy. The business unit line managers are thus responsible for identifying, managing, and reporting risk matters upstream through the management hierarchy to members of the board of directors. The board then works with the audit committee or other committee members in coordination with the chief risk officer (CRO) to manage enterprise-wide risks. Enterprise-wide risk management ensures that the organization's assets are safeguarded, its reputation is protected, and shareholder value is enhanced, all while risks are being managed. To make this happen, management must link strategy, goals and objectives, risks, individual employee performance, and organization performance.

Risk is the possibility of something adverse happening to an organization. **Risk management** is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Risk management encompasses three processes: risk assessment, risk mitigation, and risk monitoring (evaluation).

Risk management = Risk assessment + Risk mitigation + Risk monitoring

Risk assessment includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. **Risk mitigation** refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended by the risk assessment process. **Risk monitoring** is a continual process for implementing a successful risk management program. Management is responsible for determining whether the remaining risk (residual risk) is at an acceptable level or whether additional controls should be implemented to further reduce or eliminate it.

A successful risk management program relies on **critical success factors**,

- Senior management's commitment.
- The full support and participation of team members.
- The competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific process or system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization.
- The awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization.
- Ongoing evaluation and assessment of mission risks.

The fundamental reasons why organizations implement a risk management process are to minimize negative impact on an organization and to establish a sound baseline for decision making.

2.2 Risk Management Methodology

As stated earlier, risk management encompasses three processes: risk assessment, risk mitigation, and risk monitoring (evaluation).

(a) Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with a process or system. The output of the process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. Major activities in the risk assessment process include vulnerability identification, threat identification, control analysis, impact analysis, risk determination, and control recommendations.

(b) Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

(i) Risk Mitigation Options

Risk mitigation is a systematic methodology used by senior management to reduce organization risks. Risk mitigation can be achieved through any one or combination of the following risk mitigation options:

- **Risk rejection or risk ignorance.** This option is not a wise choice; all major risks must be managed.
- **Risk assumption (acceptance).** This option involves recognizing a risk and its potential consequences and accepting that risk. This usually occurs when no alternate risk mitigation strategy is more cost effective or feasible. Risk acceptance is associated with risk tolerance and risk appetite.

  To accept the potential risks and continue operating the system or **process**. At some point, management needs to decide if the operation, function, or system is acceptable, given the kind and severity of remaining risks. Risk acceptance is linked to the selection of safeguards since, in some cases, risk may have to be accepted because safeguards (countermeasures) are too expensive (in either monetary or nonmonetary terms).

  Merely selecting safeguards does not reduce risk; those safeguards need to be implemented effectively. Moreover, to continue to be effective, risk management needs to be an ongoing process. This process involves a periodic assessment and improvement of safeguards and reanalysis of risks.
- **Risk avoidance.** This option avoids the risk by eliminating the cause and/or consequence of the risk (e.g., add controls that prevent the risk from occurring, remove certain system functions, or shut down the system when risks are identified). Risk avoidance is appropriate when it is possible to reduce either the severity or the frequency of a risk.
- **Risk reduction (limitation).** This option limits the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, and detective controls) or by authorizing operation for a limited time during which additional risk mitigation by other means is put into place. This option is also called risk reduction because it affords an opportunity to decrease the likelihood that a risk will occur.
- **Risk transfer.** This option transfers the risk by using other ways to compensate for the loss, such as purchasing insurance or coinsurance, or outsourcing. It is finding another person or organization that can manage the project risk(s) better. Risk transfer is appropriate for a risk with a low expected frequency and a high potential severity. Risk protection is insurance against certain events. It involves doing something to allow the project to fall back on additional or alternate resources, should the scheduled resource(s) fail.
- **Risk contingency.** This option involves proper planning to define the necessary steps needed if an identified risk event should occur
- **Risk compliance.** This option involves complying with all applicable laws and regulations in a timely and proper manner in order to reduce compliance risk.

(ii) Residual Risk

Organizations can analyze the extent of the risk reduction generated by new or enhanced controls in terms of the reduced threat likelihood or impact. The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no system or process is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

Several equations are available to express residual risks:

Residual risks = Total risks – Mitigated risks

Residual risks = Potential risks – Covered risks

Residual risks = Total risks – Control measures applied

Residual risks = Potential risks – Countermeasures applied

Residual risks = Uncovered or Unaddressed risks

Implementation of new or enhanced controls can mitigate risk by:

- Eliminating some of the system's vulnerabilities (flaws and weaknesses), thereby reducing the number of possible threat source/vulnerability pairs.
- Adding a targeted control to reduce the capacity and motivation of a threat source (e.g., if technical controls are expensive, then consider administrative and physical controls).
- Reducing the magnitude of the adverse impact (e.g., limiting the extent of a vulnerability or modifying the nature of the relationship between the information technology [IT] system and the organization's mission).

If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

(c) Risk Monitoring

Risk monitoring or risk evaluation, the third and final process of risk management, is a continual evaluation process since change is constant in most organizations. Possible changes include:

- New businesses are acquired.
- New products are introduced.
- New services are provided.
- Networks are updated and expanded.
- Network components are added or removed.
- Applications software is replaced or updated with newer versions.
- Personnel changes are made.
- Security policies are updated.

These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk monitoring process is ongoing and evolving.

2.3 Various Types of Risks

The CRO must identify as many risk types as possible from the following 26 types of risks covering both current and potential risks. The CRO must evaluate each risk alternative for satisfying business requirements for the following risk types. The evaluator reviews each risk to determine

the overall impact of significant variations from the original assumptions on which the expected success of the alternative is based.

This section discusses 26 types of risks and suggests best practices to reduce such risks. Most of these risks are interrelated and interconnected and have a magnifying effect. For example, legal risk and regulatory risk magnify the reputation (image) risk of an organization. Some risks have a cascading effect—for example, noncompliance with contractual terms and conditions can lead to financial risk (i.e., loss of money due to payment of penalties) and legal risk (lawsuits resulting from violation of contractual rights). Therefore, these 26 risk types should be viewed from a total business context rather than on a piecemeal basis.

Four common best practices applicable to each type of risk include:

1. Acquiring traditional and nontraditional insurance coverage to protect tangible and intangible assets.
2. Conducting surveys of employees, customers, suppliers, and the industry.
3. Performing benchmarking studies to understand existing and new risks better.
4. Keeping the chain of knowledge strong and current through all employees continuously acquiring knowledge, skills, and abilities (KSAs).

(a) Human Capital Risk

Human capital (people) risk is very significant and the most risky one to watch for. Some causes of human capital risk are due to employee carelessness, fatigue, memory lapses, inattention, destructive mind (sabotage), collusion, unacceptable and uncontrolled behavior with negative attitudes, and disgruntled, unmotivated, and unhappy employees. A subtle cause includes cultural risk resulting from workforce diversity. Human resource (HR) management can play an important role in managing and controlling people risks.

A major risk item in the people risk category results from using ineffective pre-employment screening practices and improper employee reference-checking practices. If these practices are not conducted safely (i.e., legally and ethically), they can lead to potential legal risks in the form of discrimination, retaliation, and defamation lawsuits.

The goal is to conduct these screening practices without jeopardizing employees' privacy and legal rights. The scope of these practices includes hiring new employees (i.e., checking for education, work experience, work habits, and reasons for leaving) and talking about former employees to prospective employers. Furthermore, if screening practices are not conducted at all or are conducted negligently, they can lead to hiring incompetent employees with poor performance records, misconduct (e.g., sexual harassment), and the threat of workplace violence, theft, and fraud possibility.

The 14 best practices to reduce people risks are listed next.

1. Install a chief HR officer.
2. Perform employee background checks.
3. Establish policies, controls, and procedures approved by the legal department to ensure consistency and fairness in handling employee reference requests (i.e., giving and getting references).

4. Balance between getting too much information and too little information when obtaining references about prospective employees.
5. Balance between giving too much information and too little information when responding to a reference request about former employees.
6. Provide training, development, and educational programs or courses to employees taught by training consultants or corporate university staff.
7. Install coaching and mentoring methods.
8. Establish individual and/or group incentives.
9. Provide fair and equitable pay and salaries.
10. Respect individuals while keeping diversity in mind.
11. Empower employees.
12. Achieve a ranking as one of the best places to work.
13. Installing a chief learning officer to improve employees' performance and productivity.
14. Conduct human capital audits, special management reviews, and self-assessment reviews periodically and proactively to reduce people risks.

(b) Risk Caused By Management

If people are the major root cause of most problems in an organization, managing is next in the line because managing is done by and through people. **Risks** stems from the inability and incompetence of managers and executives in controlling risks and in managing and implementing new programs, new projects, new business acquisitions, new products, new policies, new procedures, new processes, and new technology. These risk also come from not exhibiting leadership skills.

There are five best practices to reduce risks caused by management:

1. Install a general manager for each business unit or division.
2. Perform basic management functions, such as plan, direct, organize, and control tasks.
3. Learn and apply hard and soft skills.
4. Learn time management and leadership skills.
5. Conduct management audits, special management reviews, and self-assessment reviews periodically and proactively to reduce risks.

(c) Strategic and Business Risk

Strategic and business risk arises from not executing the business strategic plan properly and timely and when goals of managers and nonmanagers goals are incongruent with that of the organization. It also arises from changes in the internal and external environment. It is a big risk facing an organization due to significant impact on its mission.

There are five best practices to reduce strategic and business risks:

1. Install a chief strategist.
2. Develop a strategic management process.

3. Performing management functions, such as plan, organize, direct, and control tasks.
4. Learn and apply hard and soft skills.
5. Conduct strategic management process audits, special management reviews, and self-assessment reviews periodically and proactively to reduce strategic risks.

(d) Financial and Economic Risk

Financial and economic risk arises from many sources since most corporate risks eventually are translated into money so senior management can understand the risks better. For example, a financial risk is that cash inflows and outflows will not be synchronized.

Sources of financial and economic risk include:

- Interest rate risk resulting from changes in interest rates.
- Credit risk resulting from changes in credit ratings for bonds.
- Exchange rate risk resulting from changes in foreign currency exchange rates.
- Investment risk resulting from off–balance sheet accounting practices (a hidden financial risk).
- Financial reporting risk resulting from financial restatements or misstated financial results.
- Fraud risk resulting from misconduct of managers, nonmanagers, and outsiders (e.g., customers, suppliers and vendors).
- Mergers and acquisition risks resulting from not executing the merger or acquisition properly or ethically, leading to penalties and punishments.
- Tax risk resulting from misinterpretation of the tax code, paying less taxes than what are required, or taking deductions that are not allowed by the tax code, resulting in a tax liability.
- Revenue risk resulting from overstated reporting of sales, management misdirected sales, and errors in sales reporting due to improper sales cutoffs.
- Cost risk from project cost overruns due to low estimates at the start and unexpected additional costs later.
- Speculative risk, such as hedging techniques and use of derivatives.
- Audit risk resulting from the inability of the auditor to detect fraud, not considering the risks the audited organization is facing, issuing an incorrect opinion on the financial statements, and conducting the audit work negligently and unprofessionally.
- Liquidity risk resulting from the inability to pay bills and meet other financial obligations when due.
- Market risk, which is the part of an investment security's risk that cannot be eliminated by diversification.
- Portfolio risk, which is connected with an investment when it is held in combination with other assets.
- Leverage risk resulting from excessive debt.

The seven best practices to reduce financial risks are listed next.

1. Install a chief financial officer (CFO).
2. Develop financial policies, procedures, and standards.

3. Provide honest financial reporting with integrity attached.
4. Conduct training classes on tax laws and code.
5. Use forensic accounting and auditing techniques to detect and investigate fraud.
6. Develop a culture of controls.
7. Conduct financial audits, management reviews, and control self-assessment reviews periodically and proactively to reduce financial risks.

(e) Product and Service Quality Risk

Quality risk results from producing inferior-quality products, which, in turn, increases warranty costs and product recall costs. Risk also results from delivering poor-quality services to customers.

The five best practices to reduce product quality risks include:

1. Install a chief quality officer.
2. Implement ISO 9000 and 14000 Series Standards and Six Sigma approaches.
3. Install statistical process control techniques.
4. Implement quality management tools.
5. Conduct product and service quality audits, management reviews, and quality self-assessment reviews periodically and proactively to improve product and service quality.

(f) Production and Process Risks

Production risk results from not adhering to product design specifications and not following the generally accepted world-class manufacturing best practices. There could be a mismatch between the changes to engineering drawings (blueprints) and the final product design specifications. Production risk also includes manufacturability risk, ignoring product safety requirements, manufacturing errors, delays due to unavailability of materials, and disruption in the supply chain. Purchasing risk, which is part of production risk, results from purchasing wrong materials and parts, buying materials and parts that are of inferior quality, or buying more quantity than what is needed. Processes are used to manufacture a product in that process design will affect the product design and vice versa.

The eight best practices to reduce production and process risks are listed next.

1. Install a chief manufacturing officer.
2. Design for manufacturability (i.e. less waste and no product recalls).
3. Design for quality improvement and cost reduction.
4. Design for green environment (i.e. more recycling and less pollution).
5. Design for safety (i.e., no harm or injury to people).
6. Establish long-term contracts with suppliers.
7. Conduct training classes for production staff and product engineers.
8. Conduct operations audits, management reviews, and self-assessment reviews periodically and proactively to reduce production and process risks.

(g) Service and Process Risk

Service risk results from providing poor or delayed service to customers, leading to dissatisfied and eventually lost customers. The net result is increased warranty costs and service cost refunds. Processes are used to deliver a service in that process design will affect the service design and vice versa.

The four best practices to reduce service risks are listed next.

1. Install a chief service officer.
2. Implement service industry standards.
3. Conduct benchmarking studies.
4. Conduct service audits, management reviews, and self-assessment reviews periodically and proactively to reduce and process risks.

(h) Organizational Risk

Organizational risk is the mismatch between organizational structure and business strategy. It also deals with whether management is forward looking or not or whether organizational culture meets the competitive environment. Organizational risk can also result from goal-incongruent behavior of employees, improper reporting relationships, and unclear lines of responsibility and accountability.

The six best practices to reduce organizational risks are listed next.

1. Install a chief organization development officer.
2. Cultivate corporate culture.
3. Designing proper organizational structure and reporting relationships.
4. Encourage innovation and creativity.
5. Link the business unit/division mission and strategy to the corporate mission and strategy through active employee participation and direct involvement.
6. Conduct organizational and culture audits, management reviews, self-assessment reviews, and employee surveys periodically and proactively to reduce organizational risks.

(i) Contract Risk

Contract risk results from not complying with contractual terms and conditions, leading to default, penalties, and late deliveries. Contract risk leads to financial and legal risks.

The five best practices to reduce contract risks are listed next.

1. Install a contract officer.
2. Involving the chief legal officer and his or her staff in developing and reviewing the contracts for language, terms, and conditions.
3. Install project management controls.

4. Monitor the contractor's performance.
5. Conduct contract audits, project management reviews, and self-assessment reviews periodically and proactively to reduce contract risks.

(j) Information Risk

Information risk stems from lack of quality, objectivity, utility, and integrity in information and IT systems, whether manual or automated. One example is that old technology will cease to meet system requirements at some point during the system life. Another example is using inappropriate hardware and software technologies and architectures. Information risk also includes general and application risks resulting from inadequate controls in IT and user functions. Intelligence-based company information can be stolen to blackmail the company for money or sold to competitors for financial gain.

The seven best practices to reduce information risks are listed next.

1. Install a chief information officer.
2. Develop an IT corporate governance framework.
3. Conduct IT risk assessments and evaluations.
4. Establish general controls and application controls.
5. Comply with the Information Quality Act issued by U.S. Federal Government.
6. Install strict controls over taking company data home, even for business purposes.
7. Conduct technical IT audits; review IT general and application controls; and conduct industry surveys, benchmarking studies, special management reviews, and technical self-assessment reviews periodically and proactively to reduce information risks.

(k) Trade Risk

Trade risk results from violating transborder data flow rules and not complying with a specific country's and international trade laws and regulations. Trade risks can increase tariff and nontariff costs to the importing country.

The four best practices to reduce trade risks are listed next.

1. Involve the chief globalization officer in trade dealings.
2. Comply with the international trade laws and regulations for both importing and exporting countries.
3. Understand the global economic, political, and cultural environments.
4. Conduct trade audits, management reviews, and self-assessment reviews periodically and proactively to reduce trade risks.

WHAT ARE TRANSBORDER DATA FLOWS AND PRIVACY?

Transborder data flows can be defined as the movement and storage of data by automatic means across national or federal boundaries. These data flows deal with global privacy. International data networks, connecting thousands of terminals, make it possible to exchange all kinds of data in a minimum of time and without respecting national frontiers.

In general, such transborder activity is composed of three elements: (1) the database of origin: the initial system from where the data are communicated; (2) the transmission mechanism: a through-flow station; and (3) the database of destination: the final destination and storage of the transmitted data, ready for use. Often the flow of information passes through several stations. For instance, if the destination country has no facilities to process the information, the data are first sent to another country.

Data should not be encrypted when it is flowing over some borders. One approach taken is to transmit a copy of such data unencrypted along with the encrypted data without detracting from the ability of the telecommunications system to preserve the data's integrity.

(l) Control Risk

When controls are lax and not followed, fraudulent activities can take place, and employees may take advantage of system weaknesses. Proper design and implementation of effective controls can reduce risks.

The five best practices to reduce control risks are listed next.

1. Install a chief audit executive (CAE) to conduct internal audits within the company to evaluate and monitor the effectiveness of control systems.
2. Installing a controller position in business units or divisions for establishing and monitoring the effectiveness of accounting controls.
3. Implement controls, such as directive, preventive, detective, corrective, and compensating controls.
4. Motivate and educate employees to reduce the temptation to perpetuate fraud and to cultivate a culture of controls.
5. Conduct control audits, management reviews, and control self-assessment reviews periodically and proactively to reduce control risks.

(m) Research and Development Risk

Research and development (R&D) risk results when R&D staff and product engineers design and develop new products without a real understanding of the marketplace and of customers' real needs. Lack of innovation or lack of encouragement to innovate also increases R&D risk.

The five best practices to reduce R&D risks are listed next.

1. Install a chief R&D officer.
2. Gather information about customer requirements through the use of voice of the customer (VOC) and quality function deployment (QFD) techniques.
3. Inform the product development team about the results of VOC and QFD.
4. Provide marketing training to R&D staff and product engineers.

5. Conduct R&D audits, management reviews, and technical self-assessment reviews periodically and proactively to reduce R&D risks.

(n) Technology Risk

Technology risk is whether the organization is using leading-edge technology or not. Technology risk can affect security risk because the technology could be new and unproven, and security may be difficult to implement with such technology. Leading-edge, bleeding-edge, cutting-edge, and whiz-bang technologies should be used with caution as they may not have real use, may not yield fair return on investment (ROI), and may cause implementation risks.

The six best practices to reduce technology risks are listed next.

1. Install a chief technology officer.
2. Separate hype from help.
3. Separate fact from opinion.
4. Deploy proven technologies.
5. Perform cost/benefit analysis, SWOT (strengths, weaknesses, opportunities, and threats) analysis, gap analysis, option analysis, and ROI analysis as part of initial justification.
6. Conduct technology audits, management reviews, and technology self-assessment reviews periodically and proactively to reduce technology risks.

(o) Digital and Security Risk

Digital risk results from Internet activities, such as cyber incidents and violation of intellectual property rights, copyrights, trademarks, and patents. **Security risk** arises when computer systems, networks, users, and outsiders are not complying with the established security policies, procedures, rules, and standards or when security policies, procedures, rules, and standards are not adequate or not communicated properly to all employees. Digital risks and security risks, which are related to each other, can lead to loss of revenues and reputation.

The 12 best practices to reduce digital and security risks are listed next.

1. Install an information security officer.,
2. Develop an IT security governance framework.
3. Involve the chief risk officer in the development and communication of digital policy.
4. Deploy proven security technologies on the Internet.
5. Conducting threat, vulnerability, and risk assessments periodically.
6. Integrate physical security, network security, personnel security, and information security across the entire organization by creating a culture of security.
7. Develop consistent security procedures across business partners, suppliers, vendors, franchisees, and customers.
8. Install preventive, detective, and corrective security controls over facilities, employees, outsiders, systems, data, and processes.

9. Communicate security policies to all employees in an easily understandable manner.
10. Penetrate computer systems with the use of red team, blue team, or white team security testing concepts.
11. Implement national and international security standards (e.g., NIST, COBIT, ITIL, EU, OECD, and ISO).
12. Conduct digital and security audits, special management reviews and investigations, and self-assessment reviews periodically and proactively to reduce digital and security risks.

(p) Project and Program Risk

Project/program risk is viewed from schedule and technical aspects. **Schedule risk** is evaluated for the extent to which a project is subject to unexpected delays in meeting the technical objectives of the system, regardless of cost. Items of concern include lack of technical skills, lack of enough user/IT staff, or lack of physical facilities. Further, delays in budgeting and acquisition cycles must be considered.

Technical risk is evaluated for the probability that a project will prove difficult to achieve all or part of the technical objectives due to unforeseen problems, regardless of cost or schedule. This includes management and user-acceptance risks as well as those of a purely technical nature. Generally, the alternative that is closest to the status quo presents the least exposure to such risks.

The six best practices to reduce project and program risks are listed next.

1. Install a project/program manager.
2. Develop work breakdown structure (WBS) techniques.
3. Use program evaluation and review technique/critical path method (PERT/CPM) project planning methods.
4. Issue regular project status reports.
5. Monitor project team member and contractor performance.
6. Conduct project audits, project management reviews, and project self-assessment reviews periodically and proactively to reduce project and program risks.

(q) Communications Risk

Communications risk is the inability of employees or management to communicate or listen effectively, which leads to wrong interpretation of information and inappropriate actions.

The five best practices to reduce communications risks are listed next.

1. Install a chief communications officer or its equivalent.
2. Develop multidimensional communication formats (e.g., top-down, bottom-up, diagonal, and horizontal directions).
3. Provide courses in effective listening and communication techniques.
4. Issue newsletters to employees to share company performance matters.

5. Conduct communication audits, management reviews, self-assessment reviews, and employee surveys periodically and proactively to reduce communications risks.

(r) Regulatory and Reputation Risk

Regulatory risk arises from noncompliance with laws and regulations, executive orders, directives, circulars, bulletins, and ordinances that could result in adverse publicity in the news media. Regulatory risk is related to reputation (image) risk in that noncompliance with laws and regulations will tarnish the reputation of an organization.

The five best practices to reduce regulatory risks are listed next.

1. Install a chief compliance officer or its equivalent.
2. Thoroughly understand the applicable laws and regulations.
3. Establish communication systems with regulators and government authorities.
4. Conduct training classes in laws and regulations.
5. Conduct compliance audits, special management reviews, and self-assessment reviews periodically and proactively to reduce regulatory risks.

(s) Environmental Risks

Environmental risks come from not complying with laws and regulations regarding water contamination and air pollution and the associated health-related problems that arise therefrom.

The four best practices to reduce environmental risks are listed next.

1. Install an environmental officer or its equivalent.
2. Understand environmental laws and regulations.
3. Implement ISO 14000 Standards and industry standards.
4. Conduct environmental audits, special management reviews, and self-assessment reviews periodically and proactively to reduce environmental risks.

(t) Outsourcing Risks

Outsourcing risks result from when the outsourced vendor delivers poor-quality products and services, delivers completed projects that do not meet requirements and specifications, and incurs cost overruns and time delays.

The five best practices to reduce outsourcing risks are listed next.

1. Establish a contract officer for outsourcing projects.
2. Develop a fully executed contract in conjunction with the corporate legal department.
3. Insert a right to audit clause in the contract.
4. Monitor the outsourced vendor with periodic progress reports and on-site visits.
5. Conduct outsourcing vendor audits, performance reviews, and vendor self-assessment reviews periodically and proactively to reduce outsourcing risks.

(u) Privacy Risk

Privacy risk originates from divulging or releasing personal financial information, personal medical information, trade secret formulas, and other sensitive information (e.g., salaries) about an individual to unauthorized parties.

The six best practices to reduce privacy risks are listed next.

1. Install a privacy officer or its equivalent.
2. Develop and communicate privacy policies that contain consequences for not complying with the policy.
3. Understand privacy laws and regulations.
4. Implement policies and procedures for controlling and releasing personal information to third parties.
5. Provide employee orientation classes by the HR department at the time of hiring.
6. Conduct privacy audits, special management reviews, and privacy self-assessment reviews periodically and proactively to reduce privacy risks.

Some U.S. privacy laws and regulations are listed next.

- Fair Credit Reporting Act, which protects consumer report information
- Gramm-Leach-Bliley Financial Modernization Act of 1999, which protects nonpublic personal information collected and used by financial institutions
- Health Insurance Portability and Accountability Act (HIPAA) of 1996, which protects health information collected by health plans, health care clearinghouses, and health care providers

The Federal Trade Commission is responsible for ensuring consumer protection and market competition.

An example of an international privacy law is the European Union's directive concerning the transfer of data over countries. The directive mandates companies engaging in transborder data flow maintain an "adequate level" of protection for such data.

(v) Implementation and Operational Risk

Implementation risk results from poor practices in installing a new business strategy, a new computer system, program, or project; establishing a new policy, procedure, or service; or assimilating a new business into an existing one. These risks also arise when a change is not properly and timely implemented. Also, when implementation efforts are inadequate, inefficient, and incomplete, operational risks will increase in that people may not use a new system or use it in a wrong way. Operational risks follow the implementation risks.

The seven best practices to reduce implementation and operational risks are listed next.

1. Install an implementation or operational officer.
2. Developing standard operating procedures and instructions for employees to follow.

3. Develop computer system design and operation manuals.
4. Perform testing, validation, and verification methods for new computer systems.
5. Provide training on how to use a new system, policy, or procedure.
6. Provide due diligence guidelines for acquiring new businesses.
7. Conduct implementation and operational audits, management reviews, and self-assessment reviews periodically and proactively to reduce implementation and operational risks.

(w) Marketing and Sales Risks

Marketing and sales risks stems from the inability to promote, advertise, and sell products to customers that scientists, researchers, and engineers have created, designed, and developed. They also include risks resulting from price fixing or disruption in the supply chain or using illegal telemarketing practices.

The seven best practices to reduce marketing and sales risks are listed next.

1. Install a chief marketing officer.
2. Gather information about customer requirements for products (i.e., use VOC and QFD techniques).
3. Inform the product development and R&D teams about the results of VOC and QFD.
4. Provide product training to marketing and sales staff.
5. Integrate marketing and sales functions.
6. Establish a chief telemarketing officer.
7. Conduct routine marketing and sales audits, customer perception audits, special management reviews, and self-assessment reviews periodically and proactively to reduce marketing and sales risks.

(x) Natural and Catastrophic Risks

Natural and catastrophic risks result from tornadoes, hurricanes, earthquakes, fire, floods, storms, rain, water leakages, power outages (e.g., blackouts and brownouts), wind-related accidents, and other emergencies.

The six best practices to reduce natural and catastrophic risks are listed next.

1. Install a contingency officer or its equivalent.
2. Develop crisis management plans.
3. Institute emergency preparedness programs.
4. Develop business continuity, contingency, and communication plans for the entire organization (i.e., Plan A, Plan B, or Plan C).
5. Acquire traditional insurance coverage.
6. Conduct catastrophic audits, crisis management reviews, emergency preparedness drills, and emergency readiness self-assessment reviews periodically and proactively to reduce nature and catastrophic risks.

(y) Legal and Reputation Risk

As with financial risks, many sources for **legal risk** exist. These include:

- Not complying with health and safety regulations (e.g., Occupational Safety and Health Act [OSHA] regulations in the United States)
- Employee and contractor sexual harassment complaints
- Employee age discrimination suits
- Inability to prevent employees from using illegal software
- Patent violations
- Contract-related lawsuits
- Product liability suits
- Product recalls
- Product tampering
- Employee criminal acts
- Conflict-of-interest situations
- Other illegal activities

Legal risk is related to **reputation (image) risk**, similar to the regulatory risk, which could result in adverse publicity in the news media subjecting the company to special investigations and government inquiries.

The seven best practices to reduce legal and reputation risks are listed next.

1. Install a chief legal officer or its equivalent.
2. Provide in-house training classes to employees by legal and HR departments to comply with applicable laws and regulations.
3. Provide guidelines on acquiring and installing software from reputable vendors.
4. Provide guidelines regarding downloading of official software.
5. Restrict employees from bringing software from their homes to work.
6. Restrict employees from taking company data and software home even for company use.
7. Conduct legal audits, illegal software audits, legal management reviews, and legal self-assessment reviews periodically and proactively to reduce legal risks.

(z) International Risk

International risk is the combination of political, economic, and cultural risks associated with conducting business in a foreign country. Political risk addresses the unstable government and asset expropriation, while economic risk deals with currency fluctuations, interest rate changes, and the like. For example, in some countries, the culture may prevent implementation of security controls because people believe in mutual trust in each other.

The four best practices to reduce international risks are listed next.

1. Install a chief globalization officer.
2. Work with government authorities in streamlining international trade laws and regulations.
3. Provide training to employees in understanding international laws, regulations, and culture.
4. Conduct global audits, global management reviews, and global self-assessment reviews periodically and proactively to reduce international risks.

2.4 Risk Management Tools

Measuring risk can be difficult. In practice, a variety of approaches are used ranging from simply adjusting costs up or benefits down, adjusting risk levels, adjusting dollar amounts, and adjusting probabilities to the use of statistical modeling and Monte Carlo simulation. A few of the more commonly used tools and techniques include business impact analysis (BIA), cost/benefit analysis, SWOT analysis (situation analysis), sensitivity analysis, fit-gap analysis, option analysis, economic analysis, expected value analysis, and subjective scoring. It is good business practice to combine quantitative methods with the qualitative techniques to obtain broad perspectives and comprehensive picture of risks.

(a) Business Impact Analysis

BIA is a critical step to understanding the impact of various threats, exposures, and risks facing an organization. This analysis can be applied to any business function, operation, or mission. The results of the BIA are then integrated into business strategies, plans, policies, and procedures.

(b) Cost/Benefit Analysis

To allocate resources and implement cost-effective security controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost/benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost/benefit analysis can be qualitative and quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. A cost/benefit analysis for proposed new controls or enhanced control includes:

- Determining the impact of implementing the new or enhanced controls
- Determining the impact of **not** implementing the new or enhanced controls
- Estimating the costs of the implementation. These may include:
  - Hardware and software purchases
  - Reduced operational effectiveness if system performance or functionality is reduced for increased security

- Cost of implementing additional policies and procedures
- Cost of hiring additional personnel to implement proposed policies, procedures, or services
- Training and maintenance costs

- Assessing the implementation costs and benefits against system and data criticality to determine the importance of the organization of implementing the new controls, given their costs and relative impact.

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture. Just as there is a cost for implementing a needed control, there is a cost of not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its control implementation.

(c) SWOT Analysis

The scope of situation or SWOT analysis includes an assessment of an organization's key strengths (S), weaknesses (W), opportunities (O), and threats (T). It considers several factors, such as the firm itself, the organization's industry, the firm's competitive position, functional areas of the firm, and management of the firm.

(d) Sensitivity Analysis

Sensitivity analysis includes scenario (what-if) planning and simulation studies. Sensitivity analysis indicates how much change in outputs will occur in response to a given change in inputs. As applied to investments, it indicates how much an investment's return (or net present value [NPV]) will change in response to a given change in an independent input variable, with all other factors held constant. This technique can be used on one variable at a time or on a group of variables (sometime referred to as scenario analysis). Typically, investment returns are more sensitive to changes in some variables than to changes in others.

(e) Fit-Gap Analysis

Fit-gap analysis determines the difference between the actual outcome and the expected outcome. It asks two basic questions: how much fit is there and how much gap is there. The gap can be reduced, but not eliminated, through strategies, contingency plans, and specific action steps after identifying its root causes.

(f) Option Analysis

Options analysis is more a framework for critical thinking than a model. It requires analysts to ask if all options for managing uncertainty have been considered. Options analysis may be subdivided into sequential decision analysis and irreversible investment theory.

(g) Economic Analysis

The scope of economic analysis includes break-even analysis, capital budgeting analysis (e.g., payback period, NPV, internal rate of return [IRR], and profitability index), and financial ratio analysis, such as ROI, return on quality, return on assets, and return on sales. The analysis mainly deals with quantitative data in terms of dollars and ratios.

(h) Expected Value Analysis

Expected value analysis involves the assignment of probability estimates to alternative outcomes and summing the products of the various outcomes. For example, the price of crude oil per barrel today is $10.80 and there is a 25% probability of the price rising to $11.50 in the next year, a 25% chance it will fall to $10.50, and a 50% chance of a slight increase to $11.00. The expected value (EV) of the future price of one barrel of crude oil would be:

$$EV = 0.25 \times \$11.50 + 0.25 \times \$10.50 + 0.50 \times \$11.00 = \$11.00$$

(i) Subjective Scoring

Subjective scoring involves assigning weights to responses to questions addressing areas that may introduce elements of risk. The resulting "risk" score may be just one component of an overall subjective project or investment evaluation. Evaluation criteria are individually weighted to reflect their inherent risk. Identified risk factors should be limited to a few points for manageability and understandability and for meaningful interpretation of the results.

(j) Quantitative Methods

Quantitative methods include five specific approaches:

1. Exposure factor
2. Single loss exposure value
3. Annualized rate of occurrence
4. Probability of loss
5. Annualized loss expectancy

(i) Exposure Factor

This risk metric provides a percentage measure of potential loss—up to 100% of the value of the asset.

(ii) Single Loss Exposure Value

Single loss exposure value is computed by multiplying the asset value with the exposure factor. This risk metric presents the expected monetary cost of a threat event. For example, an earthquake may destroy critical IT and communications resources, thereby preventing an organization from billing its clients for perhaps a week—until replacement resources can be established—even though the necessary information may remain intact.

Financial losses from a single event can be devastating. Alternatively, the threat of operational errors costing individually from hundreds to a few thousands of dollars—none devastating or even individually significant—may occur many times a year with a significant total annual cost and loss of operational efficiency.

(iii) Annualized Rate of Occurrence

Threats may occur with great frequency, rarely, or anywhere in between. Seemingly minor operational threats may occur many times every year, adding up to substantial loss, while potentially

devastating threats, such as a 100-year flood, fire, or hack that destroys critical files, may occur only rarely. Annualizing threat frequency allows the economic consequences of threat events to be addressed in a sound fiscal manner, much as actuarial data for insurance enables insurance companies to provide valuable, and profitable, services to their clients.

(iv) Probability of Loss

Probability of loss is the chance or likelihood of expected monetary loss attributable to a threat event. For example, loss due to operational error may extend from a 1/10 chance of losing $10 million annually to a 1/100 chance of losing $1 billion annually, provided the right combinations of conditions are met. Note that there is little utility in developing the probability of threat events for anything but relatively rare occurrences. The annualized probable monetary loss can be useful in budgeting.

(v) Annualized Loss Expectancy

The simplest expression of annualized loss expectancy is derived by multiplying the annualized rate of occurrence (i.e., threat frequency) with the single loss exposure value. For example, given an annual rate of occurrence of 1/10 and a single loss exposure of $10 million, the expected loss annually is 1/10 × $10 million = $1 million. This value is central in the cost/benefit analysis of risk mitigation and in ensuring proportionality in resources allocated to protection of assets.

(k) Qualitative Methods

Qualitative methods include judgment and the intuitive (gut feel) approach, checklists, self-assessments, focus groups, interviews, surveys, and the Delphi technique. In the Delphi technique, subject matter experts (SMEs) present their own views of risks independently and anonymously; these views then are centrally compiled. The process is repeated until consensus is obtained. The Delphi technique is a method used to avoid groupthink, as SMEs do not meet face to face to make decisions.

2.5 Managing Corporate Risks

Five best practices should be implemented to manage corporate risks on an ongoing basis.

1. **Manage existing safeguards and controls.** The day-to-day management of existing safeguards and controls ranges from the robust access control for information assets, to enforcement of systems development standards, to awareness and management of the physical environment and associated risks. Many other essential areas of safeguard and control must be administered and practiced daily. These include, but are not limited to, personnel procedures, change control, information valuation and classification, and contingency planning.
2. **Periodically assess risks.** In order to determine whether all necessary and prudent safeguards and controls are in place and efficiently administered, associated risks must be assessed periodically, preferably with quantitative risk assessment. An insecure IT environment may appear on the surface to be securely administered, but quantitative risk assessment can reveal safeguard or control inadequacies. Effective application of the results of that assessment, through risk mitigation and associated cost/benefit analysis,

can lead to the assurance of efficient safeguard or control the organization assets and improved bottom-line performance.

3. **Mitigate risks by implementing and efficiently administering safeguards and controls.** It is important to remedy situations where risk assessment shows that safeguards or controls are not in place or are not effectively administered.
4. **Risk assessment and strategic planning.** Quantitative risk assessment, applied in the consideration of alternative strategic plans, can reveal unacceptable risks in an otherwise sound business case. Failure to assess the risks associated with alternative strategic plans can result in the implementation of plans at significant monetary loss. That loss is a consequence of being unaware of, or inadequately considering, risks.
5. **Implement an enterprise risk management (ERM) program.**

2.6 Enterprise Risk Management

ERM is prescribed as an organizational use of a risk framework. Topics such as definition of ERM, Institute of Internal Auditors (IIA) survey results, approaches to ERM, ERM tools, implementation of ERM, the role of internal auditing in ERM implementation, and the roles and responsibilities of the CRO are discussed in this section.

(a) ERM Defined

Traditionally, corporate risk management has focused on partial portfolio of risks (silo approach), specifically on financial and hazard risks. The scope was narrow, ignoring all the other risks impacting the organization. It did not exploit the natural hedges and portfolio effects in the collective. It tended to treat risk as downside phenomenon. Now ERM focuses on total portfolio of risks, including financial, hazard, strategic, and operational risks. The scope of ERM is much broader than the traditional view with the objective of creating, protecting, and enhancing shareholder value. ERM treats risk as both upside and downside phenomena since it integrates all risks.

When creating shareholder value, management needs to understand risks and opportunities go together. The key is to determine whether the potential benefits of a given opportunity exceed the risks. During this exercise, management needs to consider derisking opportunities, meaning becoming a market leader by reducing the risks. This will lead to earnings and revenue growth and expense control/reduction followed by earnings consistency from year to year.

ERM is defined as a rigorous and coordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives. This includes both upside and downside risks. ERM risks are classified as:

- **Financial risk.** These are risks arising from volatility in foreign currencies, interest rates, and commodities. They include credit risk, liquidity risk (bankruptcy risk), and market risk.
- **Hazard risk.** These are risks that are insurable, such as natural disasters, various insurable liabilities, impairment of physical assets, and terrorism.
- **Strategic risk.** This is a high-level and corporate-wide risk, which includes political risk, regulatory risk, reputation risk, leadership risk, and market brand risk. It is also related to failure of strategy and changing customer needs and business conditions.

- **Operational risk.** This is a risk related to the organization's systems, processes, technology, and people.

(b) IIA Survey Results

The Institute of Internal Auditors Research Foundation conducted a multi-industry global survey of CFOs, CAEs, chief corporate counsels, and CROs to understand trends and emerging practices in ERM.

A summary of major survey results follows.

- Key drivers of ERM are a desire for a unifying framework and corporate governance regimes.
- The top five motivating factors driving ERM activity identified were:
  - **a.** Desire for a unifying framework (more than 50% of respondents)
  - **b.** Corporate governance guidelines (38%)
  - **c.** Mandate from board of directors
  - **d.** Competitive pressures
  - **e.** Desire for earnings stability
- Organizations view ERM as a tool to help manage their most important business issues, such as corporate governance, value management, change management, capital management, and contingency planning.
- The CFO is the most likely senior executive to coordinate and oversee risk management or compliance activities (90%).
- The person responsible for overseeing ERM activities is: CAE (30%), CFO (24%), and CRO (21%).
- Organizational barriers need to be overcome to implement ERM. The top five barriers include:
  - **a.** Organizational culture
  - **b.** Unclear benefits
  - **c.** Lack of formalized process, language, and definitions
  - **d.** Organizational turf
  - **e.** Lack of tools
- More than 60% of organizations identify implementing risk management programs through a change management model (high-level key lever). Low-level use of key levers, such as personnel management or compensation, may make ERM implementation very difficult.
- Most organizations include financial or operational risks in their internal auditing plan, but less than half consider strategic risks. For example, 63% of respondents reported that the finance function had a formal risk assessment process. In contrast, only 21% of respondents reported activity related to the HR function.

- Initially ERM may be more of a management information tool than a driver of corporate performance. ERM is seen as an analytical tool rather than as a performance management system.
- A variety of tools and metrics are used, such as risk mapping or optimization software. Risk metrics includes value at risk and earnings at risk.

(c) Approaches to ERM

An ERM approach can be viewed in three dimensions. The first represents the range of organization operations, including business units or locations, starting small as pilot projects and eventually rolling out to the entire enterprise (i.e., institutionalization). The second dimension represents the sources of risk (hazard, financial, operational, and strategic). This may include property catastrophe risk and currency risk. The third dimension represents the types of risk management activities or processes (risk identification, risk measurement, risk mitigation, and risk monitoring).

Within this ERM universe, two general models have emerged that are not mutually exclusive: a measurement-driven approach and a process-control approach. A measurement-driven approach focuses on identifying the key risk factors facing an organization and understanding their materiality and probability of occurrence. Risk mitigation activities are focused on the most material risks with appropriate mitigation strategies. Specific steps in the measurement-driven model include: (1) assess risk (risk factors and profiles), (2) shape risk (impacts, mitigate, and finance), (3) exploit risk (plans and opportunities), and (4) keep ahead (monitor change and loop). A process-control approach focuses on key business processes and accompanying uncertainties in the execution of the business plan. The emphasis is on linking the process steps, reporting relationships, methodologies, and data collection and reporting to ensure informed decision making. The goal is to manage risk events by achieving consistency of application across the business process spectrum, thereby limiting the possibility of surprises. The process-control model assumes that good processes can control risks.

Some organizations are approaching ERM in two ways: push approach and pull approach. In the push approach, corporate or division management tries to implement ERM throughout the organization. In the pull approach, individual business units adopt ERM at their own pace.

Scorecards, action plans, and monitoring are part of the ERM approach. The scorecards include metrics, a time frame for managing the risk, and a link to shareholder value. Action plans include identifying a risk champion and determining milestones. Monitoring includes progress reviews and review for validity of metrics.

(d) ERM Tools

Five alternative risk-transfer tools, other than traditional insurance, typically are used.

1. **Captive insurance methods,** where a noninsurance firm is created for the purpose of accepting the risk of the parent firm who owns an insurer. Here a parent firm establishes a subsidiary (called Captive Insurance Company) to finance its retained losses. Captives combine risk transfer and risk retention.
2. **Financial insurance contracts,** which are based on spreading risk over time as opposed to across a pool of similar exposures. These contracts usually involve a sharing of the investment returns between the insurer and the insured.
3. **Multiline/multiyear insurance contracts,** which combine a broad array of risks (multiline) into a contract with a policy period that extends over multiple years (multiyear). For example, a pure risk may be combined with a financial risk.

4. **Multiple-trigger policies,** which reflect that the source of the risk is not as important as the impact of the risk on the firm's earnings. A pure risk is combined with a financial risk. The policy is triggered, and payment is made, only upon the occurrence of an adverse event. These policies are more commonly used.
5. **Risk securitization,** which involves the creation of securities such as bonds, or derivatives contracts, options, swaps, futures, which have a payout or price movement that is linked to an insurance risk. Examples include catastrophe options, earthquake bonds, catastrophe bonds, and catastrophe equity puts. This method is in common use.

(e) Implementation of ERM

Senior management support and commitment is needed to properly implement the ERM program in the organization. A dedicated group of cross-functional staff is needed to push it through the organization. Employees should see the ERM program as an enhancement to existing processes rather than as a new, stand-alone process. The implementation should proceed incrementally and leverage early wins.

Most organizations implement ERM programs incrementally. Some begin by layering additional sources of risk, one at a time, into their existing processes for risk assessment and risk mitigation. Some embrace all sources of risk at the outset but tackle the processes one at a time, with most starting with risk assessment. Others take on all risk sources and all processes, but on a small, manageable subset of their operations as a pilot project. Most organizations seek early wins that will help build momentum and confidence and promote further development toward their ideal ERM process.

(f) Role of Internal Auditing in ERM Implementation

The CAE is an ERM champion and should use risk-based audit plans that are consistent with the organization's goals. Internal auditing is the implementation arm of an ERM program. Internal auditors act as facilitators in cross-functional risk assessment workshops conducted in the business units. Best practices in running workshops include length of the workshop, preparation for it, risk agreement, capturing the discussion, software selection, anonymous voting, instantaneous reporting and feedback, and selection and training of the facilitator.

Internal auditors must be process owners and subject matter experts. Internal auditors and other employees of the organization should view ERM as a value-added activity since it is both inward looking and forward thinking.

Internal auditors should think like managers and focus on business objectives rather than an audit universe. Doing this requires new skill levels for internal auditors, including facilitation skills, skills in risk scorecards, and skills in developing risk frameworks and metrics.

Traditional audit tools, such as checklist approaches and internal control questionnaires, may not work in implementing ERM programs. Internal auditors should move away from the perception of being police officers. ERM can improve the efficiency of internal auditing function since auditors accomplish more with less.

Some organizations have set up ERM committees consisting of representatives from strategic planning, HR, internal auditing, risk management, and loss prevention.

When companies fail to manage risk, they miss opportunities and can lose shareholder value. Consequently, both internal pressures and external pressures develop to improve corporate governance. With respect to corporate governance, internal auditors can play an important role in ensuring that senior management, the audit committee, and the board of directors are fully informed of the organization's risk profiles and exposures.

(g) Roles and Responsibilities of Chief Risk Officer

As a member of the senior management team, the CRO has these roles and responsibilities:

- Monitor the entire organization's risk profile.
- Develop an enterprise-wide risk architecture or risk framework that is linked down to each business unit or division.
- Develop an inventory of risks, both current and potential, with associated trigger points or events as guidance to employees.
- Develop an inventory of controls or risk mitigation action steps to address each current and potential risk in order to bring risks to an acceptable level.
- Acquire property insurance and business insurance to protect business assets (tangible and intangible) from damage, destruction, accidents, fire, floods, theft, or loss.
- Seek alternative risk-transfer tools, as an option to traditional insurance, such as multiline or multiyear insurance, multiple trigger policies, securitization, captive insurance, and finite risk insurance policies.
- Teach business unit line managers and staff managers how to develop risk versus reward trade-offs, especially when pursuing new business opportunities.
- Anticipate potential new risks facing the organization after analyzing internal changes (e.g., new business, new products, new services, new processes, new customers, and new suppliers) as well as external changes (e.g., economic, political, technical, regulatory, and international).
- Develop organization-wide business continuity and contingency plans for addressing business disasters as well as IT disasters.
- Manage enterprise-wide risks so that senior management, the audit committee, and the board of directors do not receive any unpleasant surprises.
- Work with the internal audit department in developing audit plans to identify high-risk areas for audit.
- Work with the legal department in understanding risks arising from lawsuits filed either internally or externally.
- Conduct risk audits, special management reviews, and risk self-assessment reviews periodically and proactively to manage risks facing an organization.

(h) Conduct Risk Management Audit

Through his or her leadership skills, the CRO or equivalent position must assign proper responsibility and authority and exact clear accountability to promote a risk-acceptable mind-set in the organization. It is important to know that not all risks can be eliminated, can be known, or

can be ignored. The only thing that matters is that all risks must be controlled and managed. However, even after installing safeguards (controls), there is always a residual risk that is either accepted or self-insured.

At a minimum, the CRO or designee must conduct a risk management audit in these areas:

- Various types of business risks, such as financial risk (e.g., off–balance sheet items, swaps, options, hedge funds, and derivatives; and foreign exchange risk) and trade risks, such as increased international trade barriers and increased tariffs
- Political risk (possibility of asset expropriation by foreign governments and political instability)
- Technical risk (resulting from the use of leading-edge and bleeding-edge technologies)
- Product risk (unmet customer needs, poor design quality, and poor production quality)
- Project risk (time delays and cost overruns)
- Reputation risk (resulting from product defects, recalls, service mishaps, rumors, and bad publicity, which are reflected in lower stock prices)
- Legal risk (resulting from current and anticipated lawsuits)

In addition, the CRO or designee must issue an audit report listing findings and recommendations.

2.7 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Risk can be categorized as:
   a. Objective-subjective and perils-hazards.
   b. Objective-subjective, physical-moral-morale, and pure-speculative.
   c. Static-dynamic, subjective-objective, and pure-speculative.
   d. Objective-subjective, physical-moral-morale, pure-speculative, and perils-hazards.

2. The three **most** commonly used methods of loss control are:
   a. Risk retention, risk avoidance, and risk transfer.
   b. Self-insurance, diversification, and risk transfer.
   c. Frequency reduction, severity reduction, and cost reduction.
   d. Insurance transfers, frequency reduction, and severity reduction.

3. Self-insurance differs from the establishment of a reserve fund in that:
   a. Establishing a reserve fund is a form of risk retention.
   b. Self-insurance involves prefunding of expected losses through a fund specifically designed for that purpose.
   c. Self-insurance requires the existence of a group of exposure units large enough to allow accurate loss prediction.
   d. Self-insurance requires the formation of a subsidiary company.

4. The purchase of insurance is a common form of:
   a. Risk retention.
   b. Risk transfer.
   c. Risk avoidance.
   d. Loss control.

5. Which of the following **best** represents the fit-gap analysis as a risk management tool?
   a. This analysis determines the difference between the actual outcome and the expected outcome.
   b. This analysis is used for managing uncertainty as it may be subdivided into sequential decision analysis and irreversible investment theory.
   c. This analysis deals with quantitative data in terms of dollars and ratios.
   d. This analysis involves assigning weights to responses to questions addressing areas that my introduce elements of risk.

6. Which of the following financial and accounting practices is **not** a risk for public corporations?
   a. Financial engineering
   b. Earnings management
   c. Creative accounting
   d. Off-the-books accounts

7. Which of the following has been determined to be a **reasonable** level of risk?
   a. Minimum risk
   b. Acceptable risk
   c. Residual risk
   d. Total risk

8. Which of the following enterprise risk management (ERM) frameworks address market risk?
   a. Strategic risks
   b. Operational risks
   c. Financial risks
   d. Hazard risks

9. The scope of enterprise risk management (ERM) should encompass which of the following?

I. Hazards

II. Opportunities

III. Strengths

IV. Weaknesses

a. I only

b. II only

c. I and II

d. III and IV

10. Which of the following is **best** to manage the enterprise-wide risk management program?

a. Chief risk officer

b. Board of directors

c. Chief financial officer

d. Chief governance officer

DOMAIN 3

Organizational Structure, Business Processes, and Risks (15–25%)

3.1 Risk/Control Implications of Different Organizational Structures

Organizations with common characteristics and classifications and different organization charts are discussed in this section.

(a) Organization Defined

(i) What Is an Organization?

Organization and management theorist Chester Barnard defines an organization as "a system of consciously coordinated activities or forces of two or more persons." In other words, when people gather together and formally agree to combine their efforts for a common purpose or goal, an organization is the result.

The purpose of the management process is to achieve organizational objectives in an effective and efficient manner. According to Edgar Schein, a prominent organizational psychologist, all organizations share four characteristics (see Exhibit 3.1).

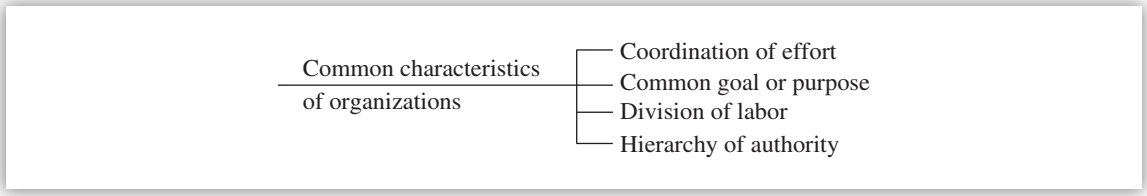


EXHIBIT 3.1 Common Characteristics of Organizations

Coordination of effort is based on the idea that two heads are sometimes better than one. Individuals who join together and coordinate their mental and/or physical efforts can accomplish great things. There is a synergy in that coordination of effort multiplies individual contributions.

Common goal or purpose gives organization members a rallying point. Coordination of effort is enhanced when employees join together to strive for something of mutual interest.

Division of labor breaks complex tasks into specialized jobs so those employees become more proficient by repeatedly doing the same specialized task.

Hierarchy of authority is needed to see that the intended goals are carried out effectively and efficiently. Authority is the right to direct the actions of others. People who promote flatter organizational structure (fewer levels of management) do not favor the traditional hierarchy of authority. However, there are people who encourage hierarchy of authority, as shown in Exhibit 3.2.

Proponents of flatter organizations	Proponents of hierarchy of authority
Fewer levels of management	Hierarchy is the most efficient, the hardiest, and the most natural structure
Hierarchy connotes bureaucracy	
Managerial hierarchy kills initiative and crushes creativity	Hierarchy can release energy and creativity, rationalize productivity, and improve morale
Speed up communications	

EXHIBIT 3.2 Proponents of Flatter Organizations and of Hierarchy of Authority

(ii) Classifying Organizations

Organizations can be classified according to their intended purposes. Four categories exist, although some large and complex organizations have overlapping categories. These categories include: (1) business organizations, (2) nonprofit service organizations, (3) mutual-benefit organizations, and (4) commonweal organizations. The primary goals of these organizations are described next.

- **Business organizations.** These organizations must make a profit to survive. The focus on satisfying the demand for products and services and earning profits.
- **Nonprofit service organizations.** Here the focus is on service, not profits. Specific service is the goal as long as the organization is solvent. These organizations have greater pressure to operate more efficiently in light of limited funds available. Such organizations serve a specific segment of society.
- **Mutual-benefit organizations.** For these organizations (e.g., a labor union or other association), the focus is on serving members' needs. Individuals join together to press for their own self-interest. Such organizations have greater pressure to operate effectively and efficiently to survive. Examples include professional associations such as Institute of Internal Auditors and unions.

- **Commonweal organizations.** Here the focus is on offering standardized public services without attempting to earn a profit. Such organizations (e.g., fire and police departments and public schools) serve all segments of society. Their great size makes them unwieldy and difficult to manage.

(iii) Organization Charts

An organization chart is a visual display of an organization's structural skeleton. Such charts show how departments are tied together along the principal lines of authority. They show reporting relationships, not lines of communication. Organization charts are tools of management to deploy human resources (HR) and are common in both profit and nonprofit organizations.

Every organization chart has two dimensions—vertical hierarchy and horizontal hierarchy—and two types—formal and informal, as shown in Exhibit 3.3.

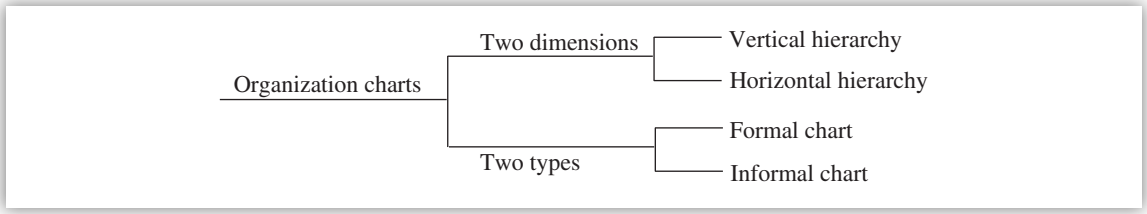


EXHIBIT 3.3 Organization Charts

A typical organization chart, displaying the managerial pyramid, will have two dimensions: horizontal and vertical. These dimensions represent the division of labor and chain of command respectively.

Vertical hierarchy establishes the chain of command, or who reports to whom. It does not show responsibilities, cannot show informal organization, and cannot show all lines of communication. A person with a lower job rank may be shown at a higher level on the chart (e.g., administrative secretary or assistant).

Horizontal hierarchy establishes the division of labor and specialization, such as marketing, production, and finance. Generally, specialization is achieved at the expense of coordination when designing organizations. A workable balance between specialization and coordination can be achieved through contingency design. The horizontal hierarchy does not show responsibilities, cannot show informal organization, cannot show all lines of communication, and does not show reporting channels or hierarchy of authority. A person with a lower job rank may be shown at a higher level on the chart (e.g., administrative secretary or assistant). Networking is accomplished through horizontal hierarchy where the interaction of persons of equal status is taking place for the purpose of professional or moral support.

The **formal chart** is the documented, official map of the company's departments with appointed leaders who get things done through power granted by their superiors. Formal charts include job titles.

The **informal chart** is not documented and is composed of natural leaders who get things done through power granted by peers. Informal charts do not include job titles.

KEY CONCEPTS TO REMEMBER: Organization Charts

- Job title does not necessarily indicate everything about that person's level of authority.
- Nominal power lies in formal organization charts.
- Real power lies in informal organization charts.
- Even supervisors need to use the informal power network to get things done.

The formal organization chart serves as a guideline, but it may not always keep track of changes in power relationships. One of the reasons why natural leaders evolve is that modern organizations are complex; they require the close cooperation of many people doing jobs that the formal organization chart cannot accommodate. *There is at least one person available with people skills and technical skills that make him or her a natural leader. There may be more than one informal leader; there is only one formal leader in each area of the company.*

Natural leadership is intangible. It can cause factions, but it can also build a positive team spirit. It is important for the formal leader to be tuned in to informal power to get things done. Formal leaders have the nominal power, and most subordinates obey to it. But the formal leader's job is made easier if he or she can influence the informal employee leadership network and win its support. This may even lay the foundation for establishing real rapport and motivating employees.

Management consultant Gareth Morgan made an interesting observation about organization charts.[1] He said that organization charts are useful tools, but they can also be extremely limiting because they entrench the idea that an organization is a structure that can be engineered and reengineered to produce appropriate results. A new organization chart is often seen as a solution to an organization's problems. But, more often than not, it can leave the basic problems unchanged. Morgan says, for example, that when a large bureaucracy is reshaped or downsized, the result is a smaller bureaucracy. When moved to matrix structure, the result is bureaucratic management in another form. Morgan's main concern is that this restructuring does not create an organization that can flow and self-organize along with the changes faced. The same old organization is reshaped with similar problems and weaknesses.

Organization charts, clearly defined systems, flow diagrams, and other engineered blueprints have provided effective models for systematizing organizational activity. They still do if one is organizing a routine, predictable task. However, they do not work in a new era of nonroutine, unpredictable task environments.

As information technology (IT) takes us into a world where old structures and forms of organization dissolve and at times become almost invisible, the old approach no longer works. Through the use of telephone, facsimile machines, electronic mail, computers, and video conferencing, employees and their organizations are becoming disembodied. They can act as if they are completely connected while remaining far apart. Employees can transcend traditional barriers of space and time, continually creating and re-creating themselves through changing networks of interconnection based on real-time communication. As one network comes into being, others dissolve. Organizations do not have to be organizations anymore.

[1] Gareth Morgan, *Imaginization: The Art of Creative Management* (Newbury Park, CA: Sage, 1993).

Nowadays, mechanistic thinking breaks down, and managers have to find fresh images for understanding and shaping what they are doing. Morgan suggests designing organizations as if they were spider plants or dandelion seeds blowing in the wind. He proposes that the management of change is the process of imaginization, which invites creativity.

3.2 Types of Organizational Structures

This section discusses contingency design alternatives, such as span of control, centralized and decentralized organizations, line and staff organizations, and matrix organizations. In addition, types of departmentalization and new organizational configurations are presented.

(a) Contingency Design Alternatives

Contingency design requires managers to select from a number of situationally appropriate alternatives instead of blindly following fixed principles of organization. Design alternatives include span of control, centralization and decentralization, line and staff organizations, and matrix organization (see Exhibit 3.4).

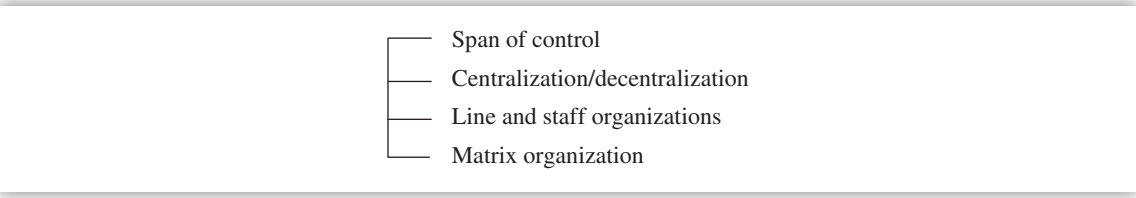


EXHIBIT 3.4 Contingency Design Alternatives

(i) Span of Control

(A) Narrow and Wide The number of people who report directly to a manager represent that manager's span of control or span of management. The optimal size of a span of control in a work area is dependent on four things:

1. The department's function
2. Organizational levels
3. Changes in the nature of the work
4. The clarity of instructions given employees

The optimal span of control is not dependent on the total number of employees in the department or company.

NARROW SPAN OF CONTROL VERSUS WIDE SPAN OF CONTROL

- A **narrow span of control** means few people to oversee, which in turn creates many hierarchical levels (tall organizations), which in turn requires many managers. The number of subordinates supervised is small. Workers are geographically dispersed.

- A **wide span of control** means many people to oversee, which in turn creates few hierarchical levels (flat organizations), which in turn requires few managers. Jobs are similar, procedures are standardized, all workers are in the same work area, and tasks are simple and repetitive. An upper limit of number of employees supervised must exist.

Obviously, a balance between too little and too much supervision is required. The ideal span of control ranges from four subordinates at the top of the organization to 12 at the lowest level. The reason for the difference is that top-level managers are supervising people and lower-level managers are responsible for supervising specific tasks.

(B) Tall and Flat A tall organization has many levels of hierarchy and a narrow span of control. A flat organization structure is one with relatively few levels of hierarchy and is characterized by a wide span of management control (see Exhibit 3.5).

Characteristics of tall organization structure	Characteristics of flat organization structure
• Tasks are highly complex and varied.	• Tasks require little direction and control of subordinates.
• Work areas are geographically dispersed.	• Employees must be able to work with little or no supervision.
• Subordinates perform distinctly different tasks.	• Departments are more timely and efficient in decision making.
• Employees are good at problem resolution due to discipline imposed by the hierarchy.	• Information flows quickly from top to bottom.
• Information flows slowly from top to bottom.	

EXHIBIT 3.5 Characteristics of Tall and Flat Organization Structures

(ii) Centralized and Decentralized Organizations

Two methods of organizations organizing are centralized and decentralized. In a **centralized organization**, decisions are made at the higher levels of management. Decisions in a decentralized organization are made at the lower levels. Authority is delegated to lower levels of the organization.

CENTRALIZATION AND DECENTRALIZATION

The extent of an organization's centralization or decentralization is determined by the span of control, the number of levels in the hierarchy, and the degree of coordination and specialization.

Centralization is typically used in those organizations that emphasize coordination of decisions that must be applied uniformly to a set of known or common problems. In planning an audit of a highly decentralized operation, an auditor assumes that the authority to make significant risk decisions has been delegated to the unit managers.

Companies that allow managers a great deal of autonomy are described as utilizing decentralized management. The factors shown in Exhibit 3.6 are considered in determining whether a centralized or decentralized design should be adopted.

Factors	Decentralization	Centralization
Number and kind of decisions:	Many unique decisions	Generic or uniform decisions
Organization culture:	Less formal	More formal
Value of uniform procedures and rules:	Rapidly changing products and industries	Slowly changing products and industries
Lower-level manager skills:	Must be generalists	Do not require as much training
Firm size and growth rate:	Larger organizations and/or rapid growth rate	Smaller organizations and/or less rapid growth rate
Strategy:	Emphasis on new product development through company research	Emphasis on production of standard products in large volume

EXHIBIT 3.6 Factors to Consider for Centralization and Decentralization

(A) Two Approaches to Achieve Decentralization **Functional decentralization** occurs when related activities or functions are grouped within an organization. For instance, all functions relating to marketing are grouped under one head. The main advantage of functional decentralization is that it allows specialists to work in areas where they contribute the most to the firm. This is very important in industries that survive mainly because of technical expertise.

However, once the specialist can make decisions independently, coordination with other areas, such as production, may suffer. Another problem is that when one group is created, it is difficult to measure the performance of the individual specialists. As the firm grows, this problem also will grow.

Divisional decentralization is the creation of units whose managers are in charge of producing and marketing a certain product, a group of related products, or activities for a geographic region. A division thus created will involve many if not all of the functions engaged in by the entire organization. Divisional decentralization results in many semi-independent units equivalent to small organizations within the larger parent.

The main advantage of divisional decentralization is that it enables decision making that is closer to the activities of the organization in contrast to decision making that arises from a central office far away. A second advantage is that responsibility can be assigned easily to the manager of a division so that his or her contribution to the company can be evaluated. A third advantage of divisional decentralization is that greater unity of command is achieved. The primary disadvantage is that this method can lead to suboptimization.

Divisional decentralization can create a feeling of autonomy in division managers that results in dysfunctional competition between them. As a result, the entire firm will suffer. Some managers will emphasize short-term gains to promote their careers to the detriment of the long-term interests of the organization.

(B) Advantages and Disadvantages of Decentralization The **advantages** of decentralization are said to arise from the greater autonomy assumed by lower-level management and workers. Top management is free to concentrate on more important problems, such as long-range planning, because lower-level management is handling many of the detailed matters on its own. The general

speed of business activity is increased since lower-level management does not have to wait for upper-level approval. Probably the greatest advantage claimed for decentralization is that it allows the freedom to think boldly and creatively, stimulates a sense of personal freedom, raises morale, and provides an excellent training ground for future top executives.

This greater autonomy also gives rise to the **disadvantages** of decentralization. With each unit making its own decisions, activities are likely to be duplicated. Normally, it would be cheaper to perform some activities centrally (e.g., finance, accounting). The managers of autonomous units may possibly ignore the advice of specialists. Decentralization can lead to suboptimization. In the interest of the whole organization, top management should install some controls to attempt to correct some of the disadvantages of decentralization.

(iii) Line and Staff Organizations

Line and staff organization structure is designed to maximize the unity-of-command principle by giving only the managers the authority to make decisions affecting those in the chain of command. There is no crossover between line and staff organization structure since each structure has its own chain of command.

Line managers have the authority to make decisions and give orders to all subordinates in the chain of command. Staff authority is generally limited to subordinates within the department. There is a natural conflict between these two parties due to power differences and different backgrounds.

One important source of conflict is the fact that line employees have formal authority while staff employees have informal power. Line managers tend to emphasize decisiveness, results, costs, and implementation, whereas staff members advise and prefer completeness, controls, adherence to policies and procedures, and systematic analysis to solve organizational problems. Staff function supports the line function but does not control it.

(iv) Matrix Organizations

In a matrix organization, people with vertical (down) and horizontal (across) lines of authority are combined to accomplish a specific objective. This design is suitable to a project environment where the project manager is responsible for completing a project without a formal line authority. Under these conditions, project managers tend to use negotiation skills, persuasive ability, technical competence, and the exchange of favors to complete a project in order to compensate for their lack of formal authority (see Exhibit 3.7).

Advantages of matrix organizations	Disadvantages of matrix organizations
Efficient use of resources	Power struggles
Project integration	Conflict
Improved information flow	Slow reaction time
Flexibility	Difficulty in controlling and monitoring tasks and people
Discipline	Overhead
Improved motivation and commitment	Stress due to dual reporting

EXHIBIT 3.7 Advantages and Disadvantages of Matrix Organizations

The matrix organization structure will likely have unity-of-command problems unless there is frequent and comprehensive communication between the various functional managers and project managers.

A large internal auditing department employs specialists in areas such as computer auditing and statistical sampling. All specialists report directly to the assistant manager for technical services. When needed on a specific audit, they report to the audit supervisor responsible for the assignment. The matrix form of organizational structure exists in relation to the specialists.

(b) Types of Departmentalization

Two common forms of integration are through the hierarchical chain of command and departmentalization. Some integration is needed to offset the negative effects of differentiation. It is through departmentalization that related jobs, activities, or processes are grouped into major organizational subunits such as departments, divisions, groups, or units.

Four basic types of departmentalization include: (1) functional departments, (2) product-service departments, (3) geographic location departments, and (4) customer classification departments (see Exhibit 3.8).

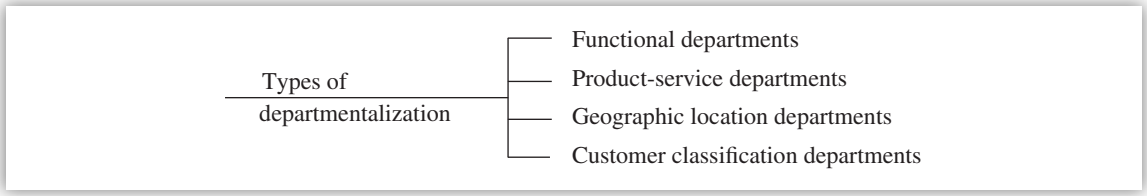


EXHIBIT 3.8 Types of Departmentalization

(i) Functional Departments

In both for-profit and nonprofit organizations, functional departments categorize jobs according to the activity performed. Manufacturing, marketing, and finance are some examples of functional departments, and the structure is popular because it permits those with similar technical expertise to work in a coordinated subunit. The structure becomes unpopular when departmental concerns tend to override more important organizational concerns. Functional departments can encourage differentiation at the expense of integration. A small, single, standard product line may be organized as a functional department, such as manufacturing, accounting, and sales. Unbroken organizational and reporting lines are indications of functional departmentalization.

CHARACTERISTICS OF ORGANIZATION STRUCTURES

- Organization structures such as functional departments, product-service departments, geographic location departments, and customer classification departments are in their pure form. In practice, a combination of these structures is found.
- Organization structures such as product-service, geographic location, and customer classification departments can create costly duplication of personnel and facilities. Functional departments do not create duplication of personnel and facilities.

(ii) Product-Service Department

In the product-service department category, a product or service, rather than a functional category of work, is the unifying theme. Ideally, those working in a product-service department have a broad business orientation rather than a narrow functional orientation. One weakness of

the product-service approach is that inefficient and costly duplication of effort may take place. A product departmentalization strategy may be good for a firm making multiple products. An example would be a computer manufacturer that organizes into mainframe computers, minicomputers, and personal computers.

(iii) Geographic Location Departments

Geographic location dictates the structure and format of the organization and emphasizes the concept that managers should be "closer to the action." Advantages include knowledge of local business and customers. Disadvantages include long lines of communication. The force behind the geographical lines is global competition. *"Think globally and act locally" is the catchphrase for companies operating in a global market.*

(iv) Customer Classification Departments

Customers have different needs and are of different types (such as business versus residential, retail versus wholesale, industrial versus commercial). The rationale behind organizing the company into customer classifications is to better service the distinctly different needs of each customer type.

(c) New Organizational Configurations

New configurations are challenging and are reshaping the traditional pyramid organization structure. These new configurations (i.e., hourglass, cluster, and network organization) not only improve the quality of work life but also improve the practice of management (see Exhibit 3.9).

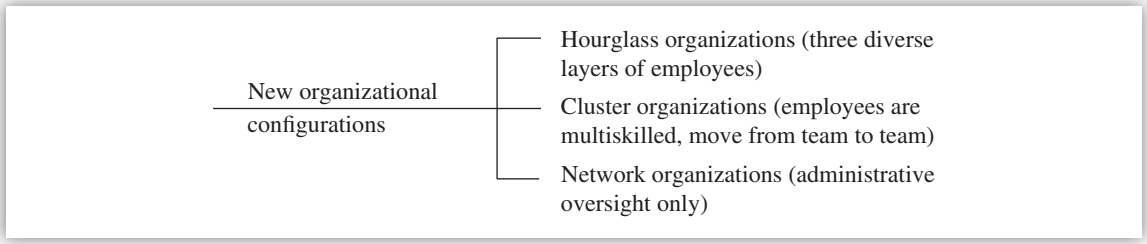


EXHIBIT 3.9 New Organizational Configurations

(i) Hourglass Organizations

The hourglass organization consists of three layers, with the middle layer distinctly pinched. The first layer is strategic management, whose members formulate a vision for the organization and makes sure it becomes a reality. The second layer is a shrunken middle management, whose members carry out a coordinating function for diverse lower-level activities. These middle managers wear different hats all the time (i.e., they handle accounting problems one day, product design issues the other day, and marketing dilemmas the next day).

TRADITIONAL PYRAMID VERSUS HOURGLASS ORGANIZATION

- Middle managers in the hourglass organization structure are business generalists. They deal with complex interfunctional problems.
- Middle managers in the traditional pyramid organization structure are business specialists. They deal with narrow and yet complex infrastructural problems.

At the bottom of the hourglass is a broad layer of technical employees who act as their own supervisors much of the time. Consequently, the distinction between supervisors and rank-and-file employees is blurred. Employees at this operating level complain about a real lack of promotional opportunities. Management should try to keep them motivated with challenging work assignments, lateral transfers, skill training opportunities, and pay-for-performance schemes.

(ii) Cluster Organizations

Teams are the primary structural unit in the cluster organization. Employees are multiskilled and move from team to team as projects dictate. Flexible work assignments are the norm. This structure promotes innovation and responsiveness. Pay for knowledge is a common practice. Motivation will be high, but so will stress levels. On the downside, job security is an issue due to constantly changing projects. Employees need to attend training programs in team building and communications.

(iii) Network Organizations

Network organizations do not produce what they sell. Hence, their only function is administrative oversight. For each organizational function (production, marketing), they have an independent contractor to handle business operations. In other words, network organizations buy a product with their own label on it and then hire other companies to distribute and sell the product.

Network organizations are "hollow corporations" built on relationships; employees spend much of their time communicating via computers, telephones, and fax machines. Advantages are lean and mean, well-run, efficient operations. Drawbacks include national security issues when operating in key industries, friction and vertical polarization (because employees are either executives or clerical workers with big pay differentials), and high turnover among nonmanagerial employees due to the fast pace of the work. Both executives and clerical employees need to attend training programs in negotiation skills, conflict management, effective communication, and handling stress.

KEY CONCEPTS TO REMEMBER: New Organizational Configurations

- The hourglass organization is a three-layer structure (strategic layer, middle layer, and operating layer) with a constricted middle layer.
- The cluster organization is a collaborative structure in which teams are the primary unit.
- In the network organization, the only function is coordination between subcontracted production and marketing operations.

3.3 Schemes in Various Business Cycles

Typical schemes in various business cycles are discussed in this section, including sales pricing objectives and policies; procurement and supply chain management; and marketing product life cycles.

(a) Sales Pricing Objectives and Policies

Pricing decisions that integrate the firm's costs with its marketing strategy, business conditions, competition, consumer demand, product variables, channels of distribution, and general resources can determine the success or failure of a business. Pricing of products or services is the cornerstone of the marketing function. *If the price is too high, buyers may purchase competitive brands leading to a loss of sales and profits. If the price is too low, profitability may suffer despite increases in sales.*

Effective pricing should consider these factors: demand influences, supply influences, and environmental influences (see Exhibit 3.10).

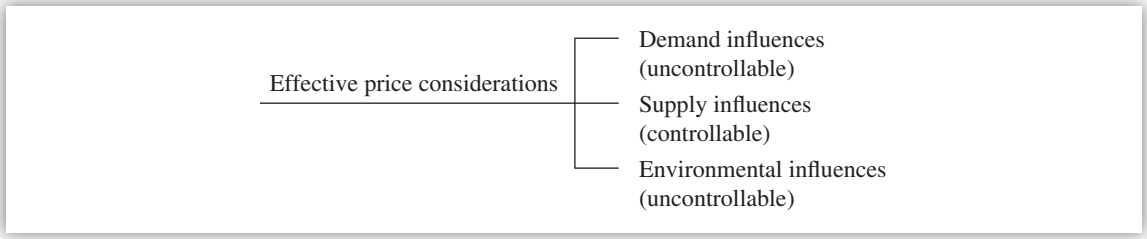


EXHIBIT 3.10 Effective Price Considerations

(i) Demand Influences

From a demand perspective, three primary considerations are: demographic factors, psychological factors, and price elasticity. **Demographic factors** include: number, location, and economic strength of potential buyers, type of consumer (i.e., resellers or final), and expected quantity of purchases by type of consumer. These demographic factors help determine market potential and are useful for estimating expected sales at various price levels.

The heart of **psychological factors** focuses on how consumers perceive various prices or price changes. It is difficult to predict how much potential buyers will be willing to pay for the product and whether potential buyers use price as an indicator of product quality. The best way to find out answers to these questions is to conduct marketing research. Although not conclusive, many research studies have found that persons who choose high-priced product categories see the consequences of a poor choice as being undesirable. They believe that quality is related to price and see themselves as good judges of product quality. In general, the reverse is true for persons who select low-priced items in the same product categories.

Both demographic and psychological factors affect **price elasticity**. Price elasticity (e) is a measure of consumers' price sensitivity, which is estimated by dividing relative changes in the quantity (Q) sold by the relative changes in price (P). This is expressed as

$$e = (\Delta Q/Q) \div (\Delta P/P) = \text{Change in quantity}/Q \div (\text{Change in price}/P)$$

Price elasticity can be estimated from historical data or from price/quantity data across different sales districts and by sampling a group of consumers from the target market and surveying them concerning various price/quantity relationships. However, bear in mind that surveying the consumers can be expensive and time consuming.

(ii) Supply Influences

Supply influences can be understood in terms of pricing objectives, costs, and nature of the product. To be effective, pricing objectives need to be derived from corporate objectives via marketing objectives as shown in Exhibit 3.11.

EXHIBIT 3.11 Pricing Objectives

Marketing research has found that the most common pricing objectives are pricing to achieve a target return on investment (ROI), stabilization of price and margin, pricing to achieve a target market share, and pricing to meet or prevent competition.

ADDITIONAL PRICING OBJECTIVES

- Target ROI and market share.
- Maximize short-run and long-run profits.
- Grow and stabilize market.
- Desensitize customers to price.
- Maintain price-leadership arrangement.
- Discourage new entrants with low prices.
- Speed exit of marginal firms.

The marketing manager focuses on multiple objectives when making pricing decisions. This becomes even more important considering that the manager does not have perfect information about cost, revenue, and market.

Every profit-oriented organization must make a profit after covering production, marketing, and administrative costs. Cost-oriented pricing is the most common approach in practice, and there are at least three basis variations: markup pricing, cost-plus pricing, and rate-of-return pricing. This is shown in Exhibit 3.12.

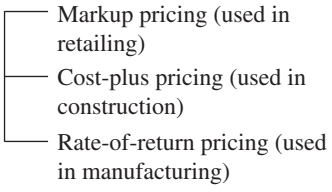


EXHIBIT 3.12 Variations of Cost-Oriented Pricing Methods

Markup pricing is used in the retail industry, where a percentage is added to the retailer's invoice price to determine the final selling price. In **cost-plus pricing**, the costs of producing a product or completing a project are totaled and profit amount or percentage is added on. It is used in job-oriented and nonroutine and difficult-to-cost advance situations, such as military installations.

In **rate-of-return or target pricing**, price is determined by adding a desired rate of ROI to total costs. Generally, a breakeven analysis is performed for expected production and sales levels and a rate of return is added on. This is shown in Exhibit 3.13.

Advantages of the cost-oriented approach	Disadvantages of the cost-oriented approach
• Simple to calculate	• Gives little or no consideration to demand factors
• Simple to understand	• Price determined by a markup or cost-plus method has no necessary relationship to what people will be willing to pay for the product
• Simple to explain	
• Simple to trace	• Places little emphasis on estimating sales volume in rate-of-return pricing
• Provides objective evidence	
• Yields a good pricing decision	• Fails to reflect competition adequately, considering the fact that costs and markups are different for each producer

EXHIBIT 3.13 Advantages and Disadvantages of the Cost-Oriented Approach to Pricing

Three important product characteristics that can affect pricing are (1) perishability, (2) distinctiveness, and (3) stage in the product life cycle. Goods that are very perishable in a physical sense (e.g., food, flowers) must be priced to promote sales without costly delays. Perishable items also include high-fashion and seasonal products since their demand is based on time. One of the primary marketing objectives of any firm is to make its product distinctive in the minds of buyers and charge higher prices. Homogeneous goods, such as bulk wheat and whole milk, are perfect substitutes for each other while most consumer goods are heterogeneous goods.

The price of a product often depends on the stage of the life cycle that a product is in and is explained in terms of price skimming and price penetration (see Exhibit 3.14).

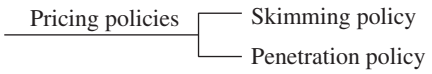


EXHIBIT 3.14 Pricing Policies

A **skimming policy** is one in which the seller charges a relatively high price on a new product. The price may be lowered later as the competition moves in. This pricing strategy is good for monopoly companies and where the demand for the product is price inelastic.

A **penetration policy** is one in which the seller charges a relatively low price on a new product to discourage competition. This pricing strategy is good where competitors can move in rapidly and where demand for the product is price elastic. Regardless of what pricing strategy is used when a new product is introduced, the price may have to be altered later to accommodate changes in the market forces.

(iii) Environmental Influences

Competitive and government regulations are two uncontrollable variables that have environmental influence on pricing. Many factors help determine whether the firm's selling price should be at,

below, or above competition. **Competitive factors** include:

- Number, size, location, and cost structure of competitors.
- Conditions of entry into the industry.
- Degree of vertical integration of competition.
- Number of products sold by competitors.
- Historical reaction of competitors to price changes.

KEY CONCEPTS TO REMEMBER: Competition and Pricing

- **Pricing a product *at* competition.** This is called going-rate pricing, which is the average price charged by the industry and is widely used for homogeneous products.
- **Pricing a product *below* competition.** This can be found in sealed-bid pricing, where the firm is bidding directly against competitors for project contracts. It is an intentional move to obtain the job contract.
- **Pricing a product *above* competition.** This pricing strategy is used when firm has a superior product or because the firm is the price leader in the industry.

Governmental regulation includes both state and federal government. The scope of state regulation includes pricing by public utility companies while the scope of federal regulation covers price fixing, deceptive pricing, price discrimination, and promotional pricing.

(iv) General Pricing Decision Model

As mentioned earlier, pricing decisions require the consideration of many factors. Peter and Donnelly[2] suggest a nine-step pricing decision model even though it is difficult to generalize an exact sequence of when each factor is to be considered. These nine steps include:

1. Define target markets.
2. Estimate market potential.
3. Develop product positioning.
4. Design the marketing mix.
5. Estimate price elasticity of demand.
6. Estimate all relevant costs.
7. Analyze environmental factors.
8. Set pricing objectives.
9. Develop the price structure.

[2] J. Paul Peter and James H. Donnelly Jr., *Marketing Management: Knowledge and Skills,* 3rd ed. (Homewood, IL: Irwin, 1992).

The *advantages* of this model are that it breaks the pricing decision into nine measurable steps, it recognizes that pricing decisions need to be integrated into overall marketing strategy, and it considers both qualitative and quantitative factors in pricing decisions.

The fact that all pricing decisions will not fit the framework just suggested is its major limitation and *disadvantage.*

(b) Procurement and Supply Chain Management

(i) Managing the Supply Chain

The supply chain is seen as equivalent to an input-transformation-output system. In this context, both customer and supplier goodwill are to be viewed as a key asset to an organization. The supply chain becomes a value chain when all of the transforming activities performed on an input provide value to a customer. The real challenge is to ensure that value is added at every step of the chain to achieve customer satisfaction. Both purchasing and the supplier play a large role in the value chain.

Managing the supply base includes integration of suppliers, involvement of suppliers, supplier reduction strategies, supplier performance, and supplier certification. The purpose of managing the supply base is to manage quality, quantity, delivery, price, and service.

Integrating suppliers means reducing or balancing the number of suppliers available so that they become part of the buyer operation to lower inventories, to increase response time and quality, and to decrease total cost.

Early **involvement of suppliers** in the product design process reduces cost, improves quality, and shortens product development cycle time. This is achieved through review of product specifications and production standards by the supplier.

CHARACTERISTICS OF SUPPLY CHAIN MANAGEMENT

Honesty, fairness, and trust have to be the driving values for effective supply management.

Supplier reduction strategies include deciding who will be single sourcing or second sourcing. Approaches to improving **supplier performance** include improved communication, early supplier involvement in the buyer product design, and measuring supplier performance indicators. Improved communication is achieved through designating one or two individuals for all communication that takes place between the buying and supplying firms and conducting supplier conferences and workshops to share information common to both parties (cost, design specifications, and profit).

The supplier performance is measured in terms of quality, delivery, service, and cost/price. **Quality measures** may include incoming defect rate, product variability; number of customer complaints, use of statistical process control, documented process capabilities, and supplier's quality philosophy. **Delivery measures** include on-time delivery, percentage and availability of product within quoted lead time, and quantity accuracy. **Service measures** include invoice accuracy and length of time required to settle claims, availability of a supply plan, and availability of engineering support. **Cost/price measures** include product

cost, price reductions, transportation cost, willingness to participate in price reviews, and minimum buy requirements.

PARADIGM SHIFT FOR AUDITORS

Internal auditors may not be comfortable with reducing or eliminating incoming inspection of goods. Doing so requires a paradigm shift on the part of auditors.

Supplier certification is a certification process conducted by the purchasing organization in that their major suppliers are certified so that shipments go directly into use, inventories, or production. The goal of certification is to reduce or eliminate incoming inspection of goods coming from a supplier by a purchaser.

Certification involves evaluating the supplier's quality systems, approving the supplier's processes, and monitoring incoming product quality. The advantages of supplier certification are increased product quality, reduced inspection costs, and reduced process variation.

(ii) Alternative Market Channels

It takes a considerable amount of time, money, and effort to set up channels of distribution. Because of this heavy commitment of resources, once decisions are made about the channel of distribution, they are not easy to retract. Yet these decisions are very critical to the success of the firm. Decisions based on inaccurate or incomplete information can be very costly. Whether a consumer good or an industrial good is concerned, channels of distribution provide the ultimate consumer or industrial user with time, place, and possession value (utility). *Thus, an efficient channel is one that delivers the product when and where it is wanted at a minimum total cost. Marketing intermediaries exist to bring about product exchanges between buyers and sellers in a reasonably efficient manner.*

(A) Marketing Intermediaries The primary role of intermediaries is to bring supply and demand together in an efficient and orderly manner (see Exhibit 3.15).

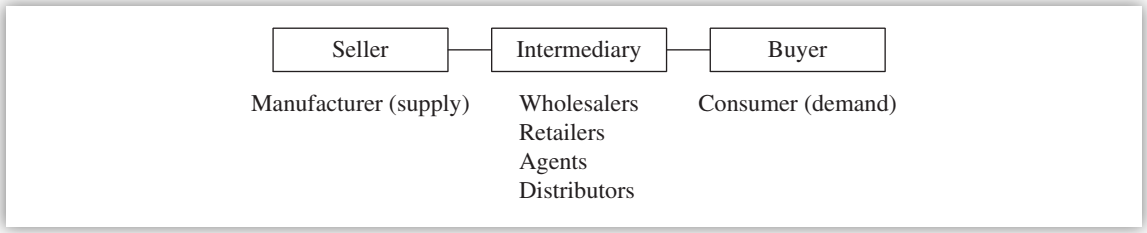


EXHIBIT 3.15 Primary Role of Intermediaries

Since it would be very difficult for each consumer to deal with each manufacturer directly for products, considering the distance between sellers and buyers and product complexity, the need for intermediaries becomes apparent. Marketing intermediaries can perform product exchange functions more cheaply and more efficiently than manufacturers can. Also, competition among intermediaries will result in lower costs to consumers. There are many types of marketing intermediaries, many of which are specialized by function and industry.

MAJOR TYPES OF MARKETING INTERMEDIARIES

Various types of marketing intermediaries are middlemen, merchant middlemen, agent, wholesaler, retailer, broker, sales agent, distributor, jobber, and facilitating agent.

(B) Channels of Distribution A channel of distribution is the integration of intermediaries through which a seller markets products to users or consumers. Agents, wholesalers, and retailers are called intermediaries, or middlemen. Channels with one or more intermediaries are referred to indirect channels. The risks assumed and the functions performed by these parties vary, as shown in the next list.

MARKETING FUNCTIONS PERFORMED IN CHANNELS OF DISTRIBUTION

- **Buying.** Purchasing products from sellers for use or for resale.
- **Selling.** Promoting the sale of products to ultimate consumers or industrial buyers.
- **Sorting.** Function performed by intermediaries in order to bridge the discrepancy between the assortment of goods and services generated by the producer and the assortment demanded by the consumer. This function includes four distinct processes: sorting out, accumulation, allocation, and assorting.
- **Accumulation.** A sorting process that brings similar stocks from a number of sources together into a larger homogeneous supply.
- **Allocation.** A sorting process that consists of building an assortment of products for use in association with each other.
- **Assorting.** A sorting process that consists of building an assortment of products for use in association with each other.
- **Concentration.** The process of bringing goods from various places together in one place.
- **Financing.** Providing credit or funds to facilitate a transaction.
- **Storage.** Maintaining inventories and protecting products to provide better customer service.
- **Grading.** Classifying products into different categories on the basis of quality.
- **Transportation.** Physically moving products from where they are made to where they are purchased and used.
- **Risk taking.** Taking on business risks involved in transporting and owning products.
- **Marketing.** Collecting information concerning such things as market conditions, research expected sales, consumer trends, and competitive forces.

Source: Dictionary of Marketing Terms (Chicago: American Marketing Association, 1988).

For convenience, the channels of distribution are classified into consumer goods and industrial goods (see Exhibits 3.16 and 3.17).

Selecting the right channels of distribution is not an easy task, considering the geography of consumers and willingness of intermediaries to accept the seller's products. For most products, intermediaries are well established, doing business for many years. Exhibit 3.18 presents six basic considerations in the initial development of channel strategy.

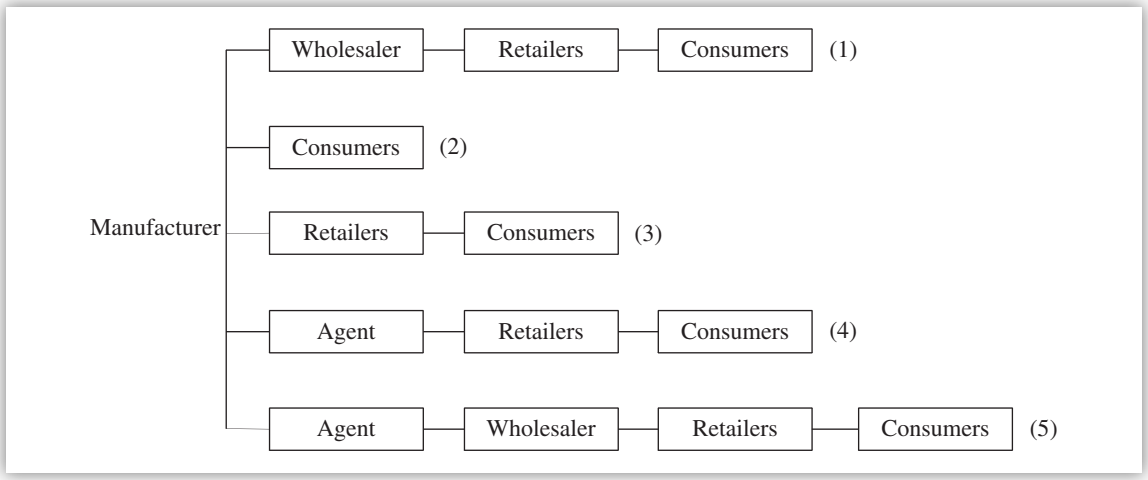


EXHIBIT 3.16 Channels of Distribution for Consumer Goods

(1) Selling a product through wholesalers to retailers to consumers is the most common channel in the consumer market.

(2) Some products are sold directly to consumers.

(3) Some private brands are sold to consumers through retailers.

(4) Some products are sold to agents to retailers to consumers.

(5) Some products are sold to agents to wholesalers to retailers to consumers when intermediaries are few in number.

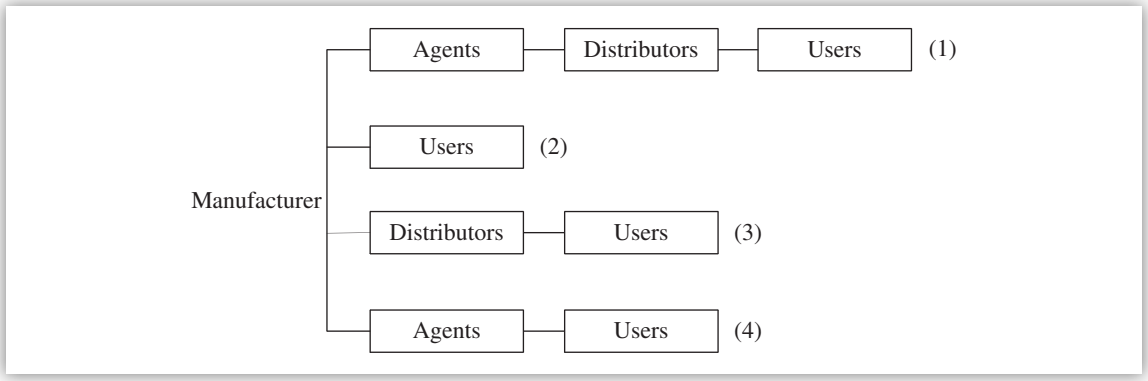


EXHIBIT 3.17 Channels of Distribution for Industrial Goods

(1) Used by a small manufacturer or when the market consists of many small customers. The manufacturer cannot afford to have a direct sales staff.

(2) Used by most manufacturers to market the product to few but large customers. The products require presale and postsale service.

(3) Used by the manufacturer when the number of buyers is large and the size of the buying firm is small.

(4) Used by small manufacturers who do not wish to have their own sales staff contract with agents. Suitable for users who are geographically dispersed.

In addition, the choice of channels can be improved by considering distribution coverage required, degree of control desired, total distribution cost, and channel flexibility. These are explained next.

(C) Distribution Coverage Required. Since the needs and expectations of the potential buyer vary, distribution coverage can be viewed as a range from intensive to selective to exclusive distribution (see Exhibit 3.19).

1. Customer characteristics include number, geographical dispersion, purchasing patterns, and susceptibilities to different selling methods.
2. Product characteristics include perishability, bulkiness, degree of standardization, installation and maintenance services required, and unit value.
3. Intermediary characteristics include availability, willingness to accept product or product line, strengths, and weaknesses.
4. Competitive characteristics include geographic proximity and proximity in outlet.
5. Company characteristics include financial strength, product mix, past channel experience, and current company marketing policies.
6. Environmental characteristics include economic conditions and legal regulations and restrictions.

EXHIBIT 3.18 Considerations in Channel Planning

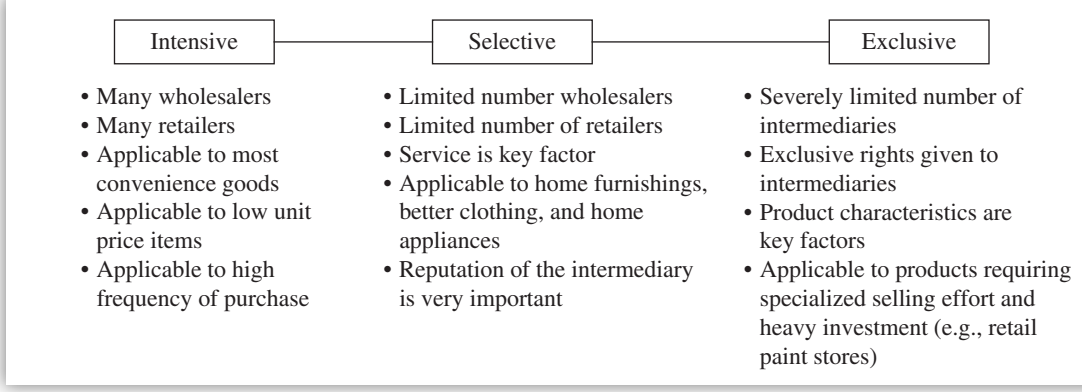


EXHIBIT 3.19 Distribution Coverage

(D) Degree of Control Desired The degree of control desired by the seller is proportional to the directness of the channel. When the market is concentrated in a limited geographic area, with many small buyers, the seller selling directly can influence the buyer significantly with his or her own policies and procedures. Control by the seller is somewhat diluted when indirect channels are used and control is more indirect rather than direct. Indirect control can be exercised through sharing promotional expenditures, providing sales training, and sharing the computer-based application system for quick response.

(E) Total Distribution Cost A total cost concept is suggested for the channels of distribution to avoid suboptimization. The concept states that a channel of distribution should be viewed as a total system composed of interdependent subsystems, with the objective to optimize total system performance. Cost minimization is a part of total system performance. A list of major distribution cost factors to be minimized follows.

- Order processing and transportation costs
- Cost of lost business (an opportunity cost due to inability to meet customer demand)
- Inventory carrying cost including storage-space charges, cost of capital invested, taxes, insurance, obsolescence, and deterioration
- Packaging and materials handling costs

Other factors that must be considered include level of customer service desired, sales volume, profit levels, and the marketing mix desired.

(F) Channel Flexibility Channel flexibility involves forecasting and/or adapting the channels of distribution in relation to changing buyer habits and population moves, such as inner cities to suburbs or north to south relocation. Change from individual stores to shopping centers and malls is also a consideration. Under these changing conditions, establishing a new channel of distribution is not that easy and takes time, money, and effort.

(iii) Selecting Intermediaries

The two basic methods of selecting intermediaries (middlemen) are ***pushing*** *and* ***pulling****.* Pushing a product through the channel means using normal promotional effort—personal skills and advertising—to help sell the whole marketing mix to possible channel members. This is a common approach with the producer working through a team to get the product to the user. By contrast, pulling means getting consumers to ask intermediaries for the product. This involves distributing samples and coupons to final consumers. If the promotion works, the intermediaries are forced to carry the product to satisfy their customer needs.

PUSH VERSUS PULL

- Pushing a product through the channel means using normal promotional effort—personal skills and advertising.
- Pulling a product means getting consumers to ask intermediaries for the product.

(iv) Managing Channels of Distribution

From a management point of view, entire channels of distribution should be treated as a social system since each party plays a defined role and each has certain expectations of the other. The interaction with each other is very critical for all parties involved, and the behavioral implications are many.

The channels of distribution do not manage themselves. Someone needs to manage or exert primary leadership in the channel. Although there are exceptions, the tendency appears to lean toward channels controlled by the manufacturer. Even though the question of managing channels of distribution is obvious, the answer is not, as indicated by the following arguments:

- Some marketers believe the manufacturer or the owner of the brand name should be the channel leader. This is because the owner has the most to lose if the system fails, has the most technical expertise, and has greater resources than others.
- Some marketers believe the retailer should be the channel captain or leader, since the retailer is the closest link to the consumer and, therefore, can judge better the consumer needs and wants.
- Some marketers argue the wholesaler should seek to gain channel control.
- Some marketers suggest that the locus of control should be at the level where competition is greatest.
- Some marketers believe that the powerful member, whether it is a manufacturer, wholesaler, or retailer, should assume channel leadership.

(c) Marketing Product Life Cycles

(i) Product Management

Product strategy is a part of the marketing mix (i.e., product, price, place, and promotion). Other parts include promotion strategy, distribution strategy, and pricing strategy.

There are many decision areas in product management, including product definition, product classification, product mix and product line, and packaging and branding (see Exhibit 3.20).

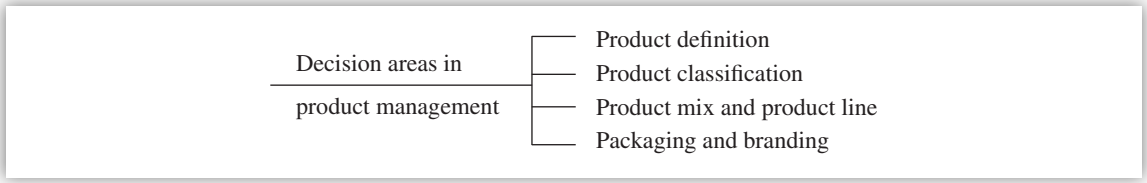


EXHIBIT 3.20 Decision Areas in Product Management

(A) Product Definition The way in which the product variable is defined can have important implications for the survival, profitability, and long-run growth of the firm. See Exhibit 3.21 for how a product can be viewed.

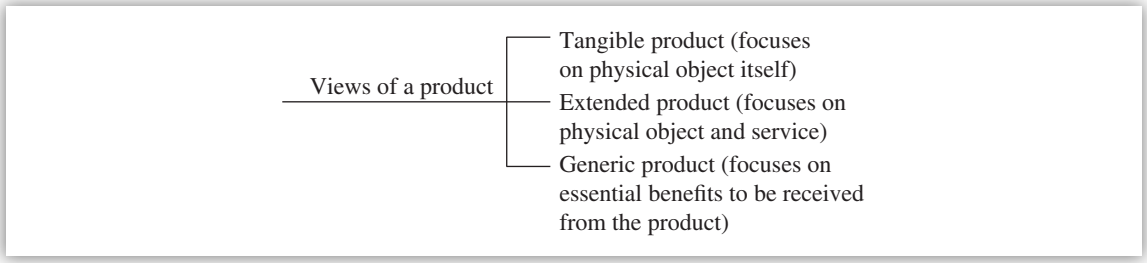


EXHIBIT 3.21 Views of a Product

A classic example of improper definition can be found in railroad passenger service, defines itself as being in the railroad business instead of in the transportation business. A reasonable definition of product is that it is the sum of the physical, psychological, and sociological satisfaction the buyer derives from purchase, ownership, and consumption.

(B) Product Classification Product classification is an analytical device to assist in planning marketing strategy and programs. A basic assumption underlying such classifications is that products with common attributes can be marketed in a similar manner. In general, products are classified according to two basic criteria: (1) end use or market and (2) degree of processing or physical transformation required.

Examples of product classification are agricultural products and raw materials, industrial goods, and consumer goods. The market for industrial products has certain attributes that distinguish it from the consumer goods market. For certain products, there are a limited number of buyers known as a **vertical market** (which means that it is narrow) because customers are restricted to a few industries, and it is deep, in that a large percentage of the producers in the market use the product. Some products, such as office supplies, have a

horizontal market, which means that the goods are purchased by all types of firms in many different industries.

(C) Product Mix and Product Line The **product mix** is the composite of products offered for sale by the firm's product line. It refers to a group of products that are closely related in terms of use, customer groups, price ranges, and channels of distribution. There are three primary dimensions of a firm's product mix, as shown in Exhibit 3.22.

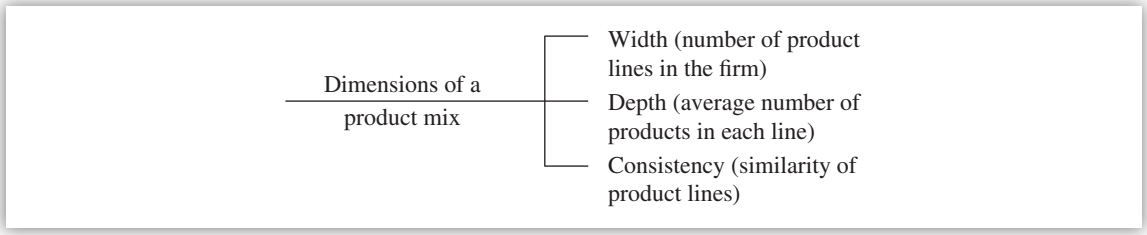


EXHIBIT 3.22 Dimensions of a Product Mix

Width of the product mix refers to the number of product lines the firm handles. **Depth** of the product mix refers to the average number of products in each line. **Consistency** of the product mix refers to the similarity of product lines. Product line plans take into account consumer evaluation of the company's products (strengths and weaknesses) and objective and accurate information on sales, profits, and market share (actual and anticipated levels).

(D) Packaging and Branding Distinctive or unique packaging is one method of differentiating relatively homogeneous products, such as toothpaste or soap. The design of packaging should focus on the size of the product, how easy it is to open, how strong the packaging should be in protecting the product, the attractiveness of the packaging, and costs.

Many companies use branding strategies to increase the strength of the product image. Factors to be considered include: product quality, whereby products do what they do very well; consistent advertising, in which brands tell their story often and well; and brand personality, where the brand stands for something unique (e.g., Xerox, and Kodak). A good brand name can evoke feelings of trust, confidence, security, and strength. Markov analysis can be used to determine the extent to which customers switch brands.

Markov analysis is useful in studying the evolution of certain systems over repeated trials. This analysis has been used, for example, to describe the probability that a machine, functioning in one period, will function or break down in another period, and to identify changes in the customer's account receivables collection experience

(E) Product Life Cycle Concepts A firm's product strategy must consider the fact that products have a life cycle—phases or stages that a product will go through in its lifetime. This product life cycle (PLC) varies according to industry, product, technology, and market. In general, product growth follows an S-shaped curve (although it is shown in Exhibit 3.23 as linear) due to innovation, diffusion of a new product, and changes in the product and the market. A typical product goes through four phases, including: (1) introduction, (2) growth, (3) maturation, and (4) decline. Some products skip a phase, such as introduction or maturity, while some products

are revitalized after decline and thereby do not go through the S-shaped pattern. Each phase is described briefly next.

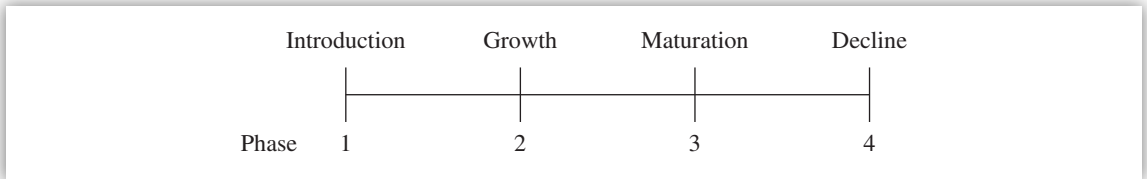


EXHIBIT 3.23 Phases/Stages of a Product Life Cycle

Introduction phase (phase 1) incurs high production and marketing costs. Profits are low or nonexistent. This phase is flat due to difficulties of overcoming buyer inertia and stimulating trials of the new product.

Profits increase and are possibly correlated with sales during the **growth stage** (phase 2) as the market begins trying and adopting the product. As the product **matures** (phase 3), profits do not keep pace with sales because of competition. Penetration of the product's potential buyers is eventually reached, causing the rapid growth to stop and level off. Price concessions, increasing product quality, and expanding advertising will be planned to maintain market share.

At some point, sales will **decline** (phase 4), and the seller must decide whether to drop the product, alter the product, seek new uses for the product, seek new markets, or continue with more of the same. Growth will eventually taper off as new substitute products appear in the market. The advice for the decline phase is not to invest in slow or negative growth or unfavorable markets but instead to pull the cash out.

Due to changing conditions, the marketing mix has to be changed in line with PLC changes. The PLC concept can help in forecasting, pricing, advertising, and product plans. The difficult part of the PLC concept is estimating the exact time periods for these four phases, as it is hard to know when one phase begins and ends. The fact that the duration of each phase varies from product to product diminishes the usefulness of the PLC concept as a marketing planning tool.

(F) Product Audit The product audit is a marketing management technique whereby the company's current product offerings are required to ascertain whether each product should be continued as is, improved, modified, or discontinued. The product manager, who is responsible for the product, should ensure that the product audit is performed at regular intervals as a matter of marketing policy. One of the major purposes of the product audit is to detect "sick" products for possible discontinuation. Some critical factors to be considered in this area are:

- **Sales trends.** How have sales moved over time? Why have sales declined?
- **Profit contribution.** What has been the profit contribution of this product to the company?
- **Product life cycle.** Has the product reached a level of maturity and saturation in the market? Has the product outgrown its usefulness? The product discontinuation issue is a hard one because it involves consideration of its negative impact on employees, keeping consumers supplied with replacement parts, disposing of inventory, and providing repair and maintenance services.

One objective of the product audit is to determine whether to modify or improve the product or to leave things as they are (status quo). Modifying the product requires changes in product

features, design, packaging, promotion, price, and channels of distribution. Product improvement suggestions often come from advertising agencies, consultants, sales staff, consumers, and intermediaries, and involve many functions, such as engineering, manufacturing, marketing, and accounting. Market research is advised when a product improvement is planned because it is not always clear as to how consumers will react to improvements or changes.

KEY CONCEPTS TO REMEMBER: Elements of Product Strategy

- An audit of the firm's actual and potential resources include financial strength, access to raw materials, plant and equipment, operating personnel, management, engineering and technical skills, and patents and licenses.
- Approaches to current markets include more of the same products; variations of present products in terms of grades, sizes, and packages; new products to replace or supplement current lines; and product deletions.
- Approaches to new or potential markets include geographical expansion of domestic sales, new socioeconomic or ethnic groups, overseas markets, new uses of present products, complementary goods, and mergers and acquisitions.
- State of competition includes new entries into the industry, product limitation, and competitive mergers or acquisitions.

(G) New Product Development Process

New Product Steps A company that can bring out new products faster than its competition enjoys many advantages and benefits. To increase speed in introducing new products, many companies are bypassing time-consuming regional tests in favor of national programs. The goal is to develop a new product right the first time. Yet the rate of new product failures is high (33–90%) and the investment is high too. There is an opportunity cost involved here due to the alternative uses of funds spent on product failures and the time spent in unprofitable product development. Marketing writers estimate that the primary reason for new product failure is the selling company's inability to match its offerings to the needs of the customer. This inability to satisfy customer needs can be attributed to three main sources.

1. Inadequacy of up-front marketing intelligence efforts
2. Failure of the company to stick close to what it does best
3. The inability to provide better value than competing products and technologies

Developing products that generate a maximum dollar profit with a minimum amount of risk is asking for the best of both worlds—an ideal solution. A more practical, systematic approach is needed to formalize the process for new product planning. New product policy guidelines should be a prerequisite for proper product planning. These guidelines should consist of procedures for various steps shown in sequence (see Exhibit 3.24).

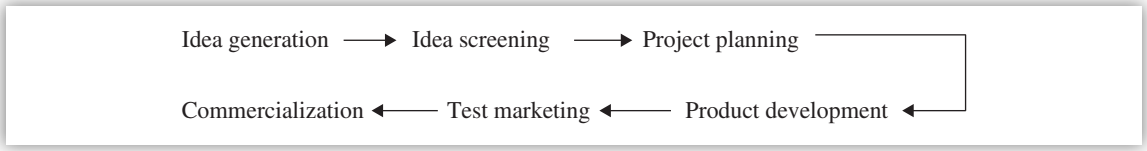


EXHIBIT 3.24 Sequence of Steps in the New Product Development Process

Causes of New Product Failure Many of the reasons for new product failure relate to execution and control problems—mostly management-oriented problems. A brief list of some of the more important causes of new product failures is presented next.

- Faulty estimates of new product potential
- Unexpected reactions from competitors
- Poor timing in the introduction of the product
- Rapid change in the market (economy) after the product introduction was approved
- Inadequate quality control
- Faulty estimates in production costs
- Inadequate expenditures on initial promotion programs
- Faulty market testing
- Improper channel of distribution

To properly address the causes of new product failures, it is important to consider both marketing research and technical research combined with gathering relevant information for decision-making purposes. For example, to calculate a ROI, one needs to know the pricing strategy to be used and the investment outlay. Similarly, one needs to estimate the magnitude of the product investment outlay and the annual cash flow in order to use the payback method, which is the rate of investment outlay to annual cash flow. The basic information required in the investment outlay includes estimates of such things as production equipment, research and development (R&D) costs, and marketing expenditures; the annual cash flow requires a forecast of quantity demanded in units and unit prices.

New Product Policy Developing a new product policy is a complicated matter since new products are the lifeblood of successful business firms. Thus, the critical product policy question is not whether to develop new products but in what direction to move. Marketing management needs to develop criteria (standards/norms) for success that new products must meet if they are to be considered candidates for launching. Possible areas for standards development include profits, costs, use of plant capacity, and market share.

There are at least 10 different ways a product can be presented as new:

1. A product performing an entirely new function
2. A product that offers improved performance of an existing function
3. A product that is a new application of an existing product
4. A product that offers additional functions
5. An existing product offered to a new market
6. A product that through lower cost is able to reach more buyers
7. An upgraded product defined as an existing product integrated into another existing product
8. A downgraded product

9. A restyled product
10. A growth vector matrix to indicate the direction in which the organization is moving with respect to its current products and markets (see Exhibit 3.25).

	Current products	**New products**
Current markets	Market penetration	Product development
New markets	Market development	Diversification

EXHIBIT 3.25 Matrix of Current/New Markets and Current/New Products

Market penetration denotes a growth direction through the increase in market share for current product markets. **Market development** refers to finding new customers for current products. **Product development** refers to creating new products to replace existing ones. **Diversification** refers to developing new products and cultivating new markets.

The 10 steps in the development of a new product policy are listed next.

1. Prepare a long-range industry forecast for existing product lines.
2. Prepare a long-range profit plan for the company, using existing product lines.
3. Review the long-range profit plan.
4. Determine what role new products will play in the company's future.
5. Prepare an inventory of company capabilities.
6. Determine market areas for new products.
7. Prepare a statement of new product objectives.
8. Prepare a long-range profit plan, incorporating new products.
9. Assign new product responsibility.
10. Provide for evaluation of new product performance.

(iv) Marketing of Services

(A) Service Characteristics The service sector of the U.S. economy has grown to such an extent that it captures about 50 cents of the consumer's every dollar. The definition of what constitutes a service remains unclear. Both products and services have these common variables that comprise the marketing mix:

- Product or service itself
- Price
- Distribution system
- Promotion
- Marketing research

Yet services possess certain distinguishing characteristics and have unique problems that result in marketing mix decisions that are substantially different from those found in communication with the marketing of goods. *These characteristics include intangibility, inseparability, fluctuating demand, a highly differentiated marketing system, and a client relationship.* Each of these characteristics is discussed next.

- **Intangibility** arises when a service firm is actually selling an idea or experience, not a product. It is often difficult to illustrate, demonstrate, or display the service in use. Examples include airline or hotel service.
- **Inseparability** arises when a service cannot be separated from the person of the seller. In other words, the service must be created and marketed simultaneously. An example is an insurance agent who is selling a policy.
- **Fluctuating demand** occurs when services fluctuate by season (tourism), days (airlines), or time of day (movie theaters). One example of stimulating demand or unused capacity is when downtown hotels (or those that are used predominantly by business travelers) offer significant discounts for a weekend stay.
- **Highly differentiated marketing systems** offer different service approaches for different services. For example, the marketing of banking or financial services requires a different approach from the marketing of computer services or airline services.
- **Client relationships** exist between the buyer and the seller, as opposed to a customer relationship. Examples include physician–patient and banker–investor relationships. The buyer follows the suggestions provided by the seller.

(B) Service Quality Poor quality of service and nonperformance are two major reasons for switching to the competition, and high price is a minor reason. Service quality is measured against performance, which can be very difficult to ascertain. In general, problems in the determination of good service quality are attributable to differences in the expectations, perceptions, and experiences regarding the encounter between the service provider and the service user.

It is easier and cheaper to keep an existing customer than to find a new one. Product quality can be measured against accepted standards, which are tangible, while service quality is measured against expected performance, which is intangible.

Service quality is the gap between expected service and perceived service. Determinants of service quality, which can help marketing managers avoid losing customers, are listed next.

- Reliability involves dependability and consistency of performance.
- Responsiveness concerns the willingness or readiness of employees to provide service.
- Competence means possession of the necessary skills and knowledge to perform the service.
- Access involves approachability and ease of contact.
- Courtesy involves politeness, respect, consideration, and friendliness of contact personnel.
- Communication means keeping customers informed in language they can understand. It also means listening to customers.
- Credibility involves trustworthiness, believability, and honesty.

- Security is the freedom from danger, risk, or doubt.
- Understanding the customer involves making the effort to understand the customer's needs.
- Tangibles include the physical evidence of the service.

(C) Overcoming the Obstacles in Service Marketing In view of the size and importance of the service economy, considerable innovation and ingenuity are needed to make high-quality services available at convenient locations for consumers. The actual services offered by service providers often fall behind the opportunities available due to five obstacles:

1. Limited view of marketing
2. Lack of competition
3. Lack of creative management
4. Concept of "no obsolescence"
5. Lack of innovation in the distribution of services

3.4 Business Process Analysis

In a manufacturing company, the scope of process analysis starts from raw materials and ends up with finished goods shipping to customers. It includes all the transformation (processing) stages, inspection steps, and transportation stages. Similarly, in a service company, the scope of process analysis starts, for example, with claims application and ends up with making payment to the claimant. The goal of process analysis is to facilitate change for improvement. Doing this requires looking at not only the individual processes where problems exist but also the upstream and downstream processes that are related to the process in question. Process improvements can be made by rearranging equipment layout, plant layout, inspection points, and testing stages with the help of motion study, material study, time study, and material handling studies. In this effort, both product processes and service processes should be examined for waste, delays, and improvement.

(a) Workflow Analysis

Workflow analysis looks at the overall flow of work to find ways of improving this flow. It can reveal value-added and non-value-added activities (e.g., waste and delays) and identify interdependence among departments. The outcome would be eliminating the non-value-added activities and waste and improving efficiency and effectiveness. Assembling tasks, whether subassembly or final assembly, and process time are value-added activities of a manufactured product, while other activities are non-value-added activities. Examples of non-value-added activities from a customer's viewpoint include inspection time, move time, reporting time, governmental compliance time, storage time, wait time, and queue time.

Workflow systems would make organizations undergo huge managerial and cultural changes, help employees apply business rules, enable process reengineering, provide parallel processing of documents, eliminate information float or overload, and ensure that established policies and procedures are followed. Workflow software allows business processes to be redesigned and streamlined and automatically routes work from employee to employee.

Interdependence means the extent to which departments depend on each other for resources or materials to accomplish their tasks. Low interdependence means that departments can do their work independent of each of other and have little need for interaction, consultation, or exchange of materials. High interdependence means departments must constantly exchange resources and materials.

Three types of interdependence influence organization structure: pooled, sequential, and reciprocal. Pooled interdependence is the lowest form of interdependence among departments. Work does not flow between units. Each department is part of the organization and contributes to the common good of the organization, but it works independently. When interdependence is of serial form, with parts or documents produced in one department becoming inputs to another department, sequential interdependence exists. Here departments exchange resources and depend on others to perform well. The management requirements for sequential interdependence are more demanding than for pooled interdependence. These requirements include coordination, communication, integrators, and task forces. The highest level of interdependence is reciprocal interdependence. This exists when the output of operation A is the input to operation B, and the output of operation B is the input back again to operation A. The outputs of departments influence those departments in reciprocal fashion. Management requirements for the complex reciprocal interdependence include greater planning, coordination, communication, permanent teams, and frequent adjustments in the work and its associated plans.

(b) Bottleneck Management

A **bottleneck** is a constraint in a facility, function, department, or resource whose capacity is less than the demand placed upon it. For example, a bottleneck machine or work center exists where jobs are processed at a slower rate than they are demanded. Another example is where the demand for a company's product exceeds the ability to produce the product.

Bottleneck influences both product profitability and product price. The contribution margin per bottleneck hour or the value of each bottleneck hour should be analyzed. This measure is better than the normal contribution margin per unit. The contribution margin per hour of bottleneck can be used to adjust the product price to better reflect the value of the product's use of a bottleneck. Products that use a large number of bottleneck hours per unit require more contribution margin than products that use few bottleneck hours per unit.

(c) Theory of Constraints

Theory of constraints (TOC) is a manufacturing strategy that attempts to remove the influence of bottlenecks on a process. According to Dr. Eliyahu M. Goldratt, TOC consists of three separate but interrelated areas: (1) logistics, (2) performance measurement, and (3) logical thinking. Logistics include drum-buffer-rope scheduling, buffer management, and VAT analysis. Performance measurement includes throughput, inventory and operating expense, and the five focusing steps. Logical thinking process tools are important in identifying the root problems (current reality tree), identifying and expanding win-win solutions (evaporating cloud and future reality tree), and developing implementation plans (prerequisite tree and transition tree).

Drum-buffer-rope scheduling is the generalized process used to manage resources to maximize throughput. The drum is the rate or pace of production set by the system's

constraint. The buffers establish the protection against uncertainty so that the system can maximize throughput. The rope is a communication process from the constraint to the gating operation that checks or limits material released into the system to support the constraint.

Buffer management is a process in which all expediting in a factory shop is driven by what is scheduled to be in the buffers (constraint, shipping, and assembly buffers). By expediting this material into the buffers, the system helps avoid idleness at the constraint and missed customer due dates. In addition, the causes of items missing from the buffer are identified, and the frequency of occurrence is used to prioritize improvement activities.

VAT analysis is a procedure for determining the general flow of parts and products from raw materials to finished products (the logical product structure). A "V" logical product structure starts with one or few raw materials, and the product expands into a number of different products as it flows through divergent points in its routings. The shape of an "A" logical product structure is dominated by converging points. Many raw materials are fabricated and assembled into a few finished products. A "T" logical product structure consists of numerous similar finished products assembled from common assemblies, subassemblies, and parts. Once the general parts flow is determined, the system control points (gating operations, convergent points, divergent points, constraints, and shipping points) can be identified and managed.

The **five focusing steps** is a process to continuously improve organizational profit by evaluating the production system and the marketing mix to determine how to make the most profit using the system constraint. The steps consist of:

1. Identifying the constraint to the system.
2. Deciding how to exploit the constraint to the system.
3. Subordinating all nonconstraints to the system.
4. Elevating the constraint to the system.
5. Returning to Step 1 if the constraint is broken in any previous step, while not allowing inertia to set in.

(d) Business Process Review

(i) Business Process Reengineering

In an effort to increase revenues and market growth, organizations are conducting business process reviews. The idea behind business process reviews, whether for a production process or a service process, is to streamline operations and to eliminate waste. The result is increased efficiencies, which can lead to greater effectiveness. A proven technique is business process reengineering (BPR), which requires big thinking and making major, radical changes in the business processes. Workflow analysis is a part of BPR.

BPR is one approach for redesigning the way work is done to support the organization's mission and reduce costs. BPR starts with a high-level assessment of the organization's mission, strategic goals, and customer needs. Basic questions are asked, such as: Does our mission need to be redefined? Are our strategic goals aligned with our mission? Who are our customers? An organization may find that it is operating on questionable assumptions, particularly in terms of the wants and

needs of its customers. Only after the organization rethinks *what* it should be doing does it go on to decide *how* best to do it.

Within the framework of this basic assessment of mission and goals, reengineering focuses on the organization's business processes: the steps and procedures that govern how resources are used to create products and services that meet the needs of particular customers or markets. As a structured ordering of work steps across time and place, a business process can be decomposed into specific activities, measured, modeled, and improved. It can also be completely redesigned or eliminated altogether. Reengineering identifies, analyzes, and redesigns an organization's core business processes with the aim of achieving dramatic improvements in critical performance measures, such as cost, quality, service, and speed.

BPR AND BPI

Techniques such as business process reengineering (BPR) and business process improvement (BPI) are used to improve efficiency, reduce costs, and improve customer service. IT is an enabler of BPR and BPI, not a substitute for them.

Reengineering recognizes that an organization's business processes are usually fragmented into subprocesses and tasks that are carried out by several specialized functional areas within the organization. Often no one is responsible for the overall performance of the entire process. Reengineering maintains that optimizing the performance of subprocesses can result in some benefits but cannot yield dramatic improvements if the process itself is fundamentally inefficient and outmoded. For that reason, reengineering focuses on redesigning the process as a whole in order to achieve the greatest possible benefits to the organization and their customers. This drive for realizing dramatic improvements by fundamentally rethinking how the organization's work should be done distinguishes BPR from BPI efforts that focus on functional or incremental improvement.

Reengineering is not a panacea. There are occasions when functional or incremental improvements are the method of choice, as when a process is basically sound or when the organization is not prepared to undergo dramatic change. When there is a need to achieve order-of-magnitude improvements, BPR is the method of choice.

(ii) Business Process Improvement

BPI should be continuous, not discrete, and it tends to be more of an incremental change that may affect only a single task or segment of the organization. The concept of fundamental or radical change is the basis of the major difference between BPR and BPI. Quite often BPI initiatives limit their focus to a single existing organizational unit. This in itself breaks one of the tenets of BPR, which is that BPR must focus on redesigning a fundamental business process, not on existing departments or organizational units. While BPR seeks to define what the processes should be, BPI focuses more on how to improve an existing process or service.

Through BPI, organizations can achieve significant incremental improvements in service delivery and other business factors (e.g., increase in employee's productivity). The expected outcomes of BPI are not as dramatic as those associated with BPR initiatives, but the process is also not as

traumatic as in achieving the radical changes seen with BPR. In many cases, incremental changes may be achieved in situations lacking the support necessary for more radical changes. Exhibit 3.26 shows the key differences between BPR and BPI.

Element	BPR	BPI
Degree of change	Radical (e.g., 80%)	Incremental (e.g., 10–30%)
Scope	Entire process	Single area, function/unit
Time	Years	Months
Driver	Business	Technology
Focus	Redefine process	Automate/eliminate the function
Work structure	Unified	Fragmented
Orientation	Outcome	Function

EXHIBIT 3.26 BPR versus BPI

BUSINESS PROCESS REENGINEERING VERSUS BUSINESS PROCESS IMPROVEMENT

- BPR focuses on achieving dramatic improvements.
- BPI focuses on achieving incremental improvements.

(e) Benchmarking

(i) Benchmarking Defined

Benchmarking is the selection of best practices implemented by other organizations. Best practices are the best ways to perform a business process. Organizational change and improvement are the major elements of benchmarking. Benchmarks are the result of a study of organizational processes. Arthur Andersen's Best Practices report identified six first-level, basic processes that define a company's operations:

1. Understanding markets and customers
2. Designing products and services
3. Marketing and selling those products and services
4. Producing what customers need and want
5. Delivering products and services
6. Providing service to customers

Supporting these basic operations, management and support processes maximize the value with the use of HR, IT, and financial/physical resources.

The best way to practice benchmarking is to:

- Analyze business processes (inventory major business processes, conduct documentary research, and attend conferences to understand new developments).
- Plan the benchmark study (define scope, request site visits, and develop a methodology for capturing the new data).
- Conduct the benchmark study (analyze best practices and identify performance gaps).
- Implement the benchmark results (incorporate best practices into business processes and reevaluate the business processes).

(ii) Types of Benchmarking

Two types of benchmarking exist: business process benchmarking and computer system benchmarking. Business process benchmarking deals with BPI and BPR to reduce costs and to improve quality and customer service. Computer system benchmarking focuses on computer hardware/software acquisition, computer system design, computer capacity planning, and system performance. Each has its own place and time.

Business benchmarking is an external focus on internal activities, functions, or operations in order to achieve continuous improvement.[3] The objective is to understand existing processes and activities and then to identify an external point of reference, or standards, by which that activity can be measured or judged. A benchmark can be established at any level of the organization in any functional area, whether manufacturing or service industries. The ultimate goal is to attain a competitive edge by being better than the best.

Value creation is the heart of organizational activity, whether in a profit or a nonprofit entity. Benchmarking provides the metrics by which to understand and judge the value provided by the organization and its resources. Benchmarking focuses on continuous improvements and value creation for stakeholders (i.e., owners, customers, employees, and suppliers), utilizing the best practices to focus improvement efforts.

Benchmarking targets the critical success factors for a specific organization. It considers the mission of an organization, its resources, products, markets, management skills, and others. It requires an identification of customer(s), whether internal or external to the organization. Benchmarking is an early warning system of impending problems and is not a onetime measurement. Benchmarking can focus on improving organization structures, analyzing managerial roles, improving production processes, and developing strategic issues.

What are the sources of information for benchmarking? Benchmarking can be done by using published materials; insights gained at trade association meetings; and conversations with industry experts, customers, suppliers, academics, and others.

(iii) When Is the Right Time for Business Process Benchmarking?

Benchmarking should be undertaken when triggers are present. These triggers can arise internally or externally in response to information needs from some other major project or issue or problem in the company. Examples of these triggers include quality programs, cost reduction

[3] C. J. McNair and Kathleen Leibfried, *Benchmarking* (New York: Harper Business, 1992).

programs, new management, new ventures, and competitive moves. Benchmarking should be done as needed, without any preconceived notions.

(iv) Reasons for Business Process Benchmarking

A company should benchmark for three reasons: (1) it wants to attain world-class competitive capability, (2) it wants to prosper in a global economy, and (3) it simply wishes to survive (desperation). A company can benchmark in six distinct ways (see Exhibit 3.27):

1. Internal benchmarking
2. Competitive benchmarking
3. Industry benchmarking
4. Best-in-class benchmarking
5. Process benchmarking
6. Strategic benchmarking

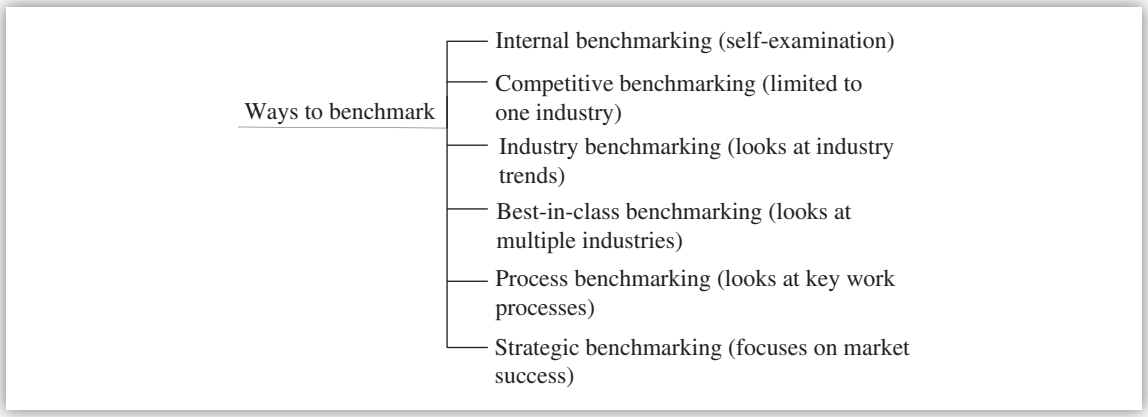


EXHIBIT 3.27 Ways to Benchmark

Internal benchmarking is the analysis of existing practices within various departments or divisions of the organization, looking for best performance as well as identifying baseline activities and drivers. Drivers are the causes of work: the trigger that sets in motion a series of actions, or activities that will respond to the requests or demands by the stockholders.

In doing internal benchmarking, management is looking downward, examining itself first before looking for outside information. Significant improvements are often made during the internal analysis stage of the benchmarking process. Value-added activities are identified and non-value-adding steps are removed from the process. Internal benchmarking is the first step because it provides the framework for comparing existing internal practices to external benchmark data. *Internal benchmarking focuses on specific value chains or sequences of driver-activity combinations.*

Competitive benchmarking looks outward to identify how other direct competitors are performing. Knowing the strengths and weaknesses of the competitors provides good input for strategic and corrective actions.

Industry benchmarking extends beyond the one-to-one comparison of competitive benchmarking to look for trends. It is still limited in the number of innovations and new ideas

it can uncover because every company is following every other company in the industry. At best, it can help establish the performance baseline or can give an incremental gain. It gives a short-run solution and a quick fix to an existing problem. However, it does not support quantum leaps or breakthroughs in performance since the comparison is limited to one industry.

Best-in-class benchmarking looks across multiple industries in search of new, innovative practices, no matter what their source. The best-in-class benchmarking is the ultimate goal of the benchmarking process. It supports quantum leaps in performance and gives a long-run competitive advantage.

Process benchmarking centers on key work processes, such as distribution, order entry, or employee training. This type of benchmarking identifies the most effective practices in companies that perform similar functions, no matter in what industry.

Strategic benchmarking examines how companies compete and seeks the winning strategies that have led to competitive advantage and market success.

WHICH BENCHMARKING DOES WHAT?

- Internal benchmarking looks downward and inward.
- Competitive benchmarking looks outward.
- Industry benchmarking looks for trends. It provides a short-run solution and a quick fix to a problem.
- Best-in-class benchmarking looks for the best all around. It provides a quantum jump in improvement.
- Process benchmarking is specific.
- Strategic benchmarking is broad with big impact.

(f) Design of Performance Measurement Systems

Performance measures should be accurately defined, analyzed, and documented so that all interested parties are informed about them. Performance standards should bring meaning to measurements. Employees who are being measured should feel that standards and specific performance measures are fair and achievable. Self-measurement may create confidence and trust, and permit fast feedback and correction from employees. But it can also lead to distortions, concealment, and delays in reporting.

One of the design objectives should be that the performance standards must be simple, meaningful, comparable, reproducible, and traceable, given similar business conditions. Care should be taken to compare items that are alike in terms of units of measurements (pounds, grams, liters, or gallons), time frames (hours or days), quantity (volume in units or tons), and quality (meeting the requirements).

During the design of performance measurements, the design team should take both human factors and technical factors into account. From a human factor viewpoint, ensure that the performance

measures are not so loose that they present no challenge or so tight that they cannot be attainable. Ideally, both subordinates and superiors must participate in identifying and developing the performance metrics. From a technical factor viewpoint, employees should be given proper tools, training, and equipment to do their job. Otherwise frustration will result. Above all, the performance measures should be based on objective measurement instead of subjective measurement to minimize human bias and suspicion of the reported measurements.

Periodically, the performance measurements should be reviewed and updated to ensure their continued applicability to the situations at hand. Evaluations of performance measures should concentrate on the significant exceptions or deviations from the standards. Therefore, exception reporting is preferred. Significant variances (deviations) require analysis and correction of standards or procedures.

The standards should match the objectives of the operation or function being reviewed. In developing standards, it is better for the auditor to work with the client than alone, with standards later validated by subject matter experts or industry experts for authentication. Usually the standards can be found in standard operating procedures, job descriptions, organizational policies and directives, product design specifications, operating budgets, trade sources, organization's contracts, applicable laws and regulations, generally accepted business practices, generally accepted accounting principles, and generally accepted auditing standards.

(g) Specific Performance Measures

Performance is the organization's ability to attain its goals by using resources in an efficient and effective manner. In this section, topics such as productivity, effectiveness, efficiency, and economy are discussed, compared, and contrasted.

(i) Productivity Defined

Productivity is the organization's output of goods and services divided by its inputs. This means productivity can be improved by either increasing the amount of output using the same level of inputs or reducing the number of inputs required to produce the output.

Two approaches for measuring productivity are total factor productivity and partial productivity. **Total factor productivity** is the ratio of total outputs to the inputs from labor, capital, materials, and energy. **Partial productivity** is the ratio of total outputs to a major category of inputs (e.g., labor, capital, or material). Productivity measurement is used to indicate whether there is a need for any improvement in the first place. It is often a part of the improvement process itself and is used to gauge whether improvement efforts are making any progress.[4] Measurement alone has a dramatic impact on productivity since the effects of feedback are so powerful. Measurement helps diagnose productivity needs and can be used to focus improvement resources on the most-needed operations. Monitoring of performance, feedback, and regular consideration of performance peaks and valleys as indicated by measurement data are powerful stimuli for change.

Productivity measurement strategies must be simple and practical and must be continually reevaluated. From a classical viewpoint, **productivity** is defined as a ratio such that the output of

[4] Robert O. Brinkerhoff and Dennis E. Dressler, *Productivity Measurement: A Guide for Managers and Evaluators,* Applied Social Research Methods Series, Vol. 19 (Newbury Park, CA: Sage, 1990).

an effort under investigation is divided by the inputs (e.g., labor and energy) required to produce the output. Examples of productivity measurement metrics are:

- Number of customers helped divided by the number of customer service representatives
- Number of pages typed divided by the number of hours of clerical time

(ii) Components of Productivity Measurement

Four components of productivity measurement exist: (1) inputs, (2) processes, (3) interim outputs, and (4) final outputs from which all measures of productivity are built (see Exhibit 3.28).

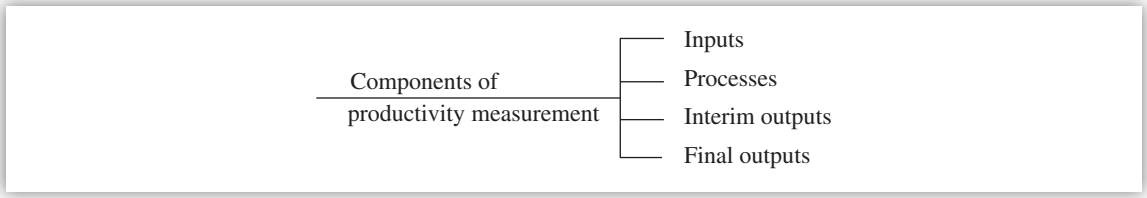


EXHIBIT 3.28 Components of Productivity Measurement

Input represents the amount of resources consumed in the production of outputs such as clerical time, budget, and labor hours. **Processes** transform inputs to final outputs through **interim outputs**. **Final output** represents some unit of production or results, such as number of contracts negotiated and amount of profit per completed contract. Both outputs and inputs must be measurable and quantifiable.

(iii) Criteria for Productivity Improvement

In addition to accuracy, four other criteria must be considered as part of the continuous process of productivity improvement: (1) quality, (2) mission and goals, (3) rewards and incentives, and (4) employee involvement (see Exhibit 3.29).

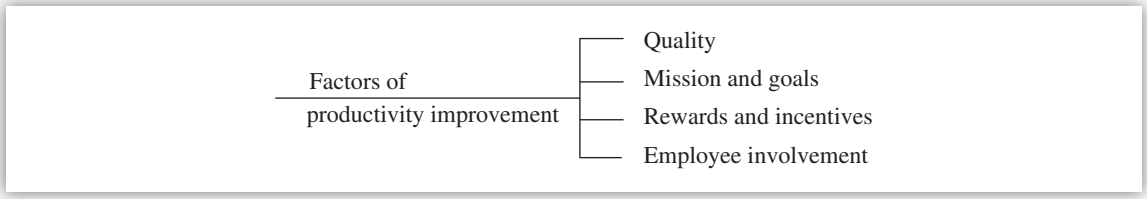


EXHIBIT 3.29 Factors of Productivity Improvement

- **Quality.** A measure that assesses only quantity of outputs can lead to reduced productivity in the long run. Both quality and quantity must be defined and measured.
- **Mission and goals.** The measure must be related to an organization's mission and strategic goals. Measures directed to products and services that are not consistent with mission and goals threaten productivity.
- **Rewards and incentives.** Measures must be integrated with performance incentives, reward systems, and practices. Measures that have no important contingencies will not work to improve productivity.
- **Employee involvement.** Employees must participate in the definition and construction of productivity measures. When lack of involvement has not resulted in commitment and

buy-in, results from the measures are not likely to be received favorably or to have any impact on future productivity.

COMMON KINDS OF CRITERIA FOR MEASUREMENT OF OUTPUTS

- Accuracy
- Timeliness
- Quantity
- Customer satisfaction
- Completeness
- Cost performance

(iv) Guidelines for Productivity Measurement

Productivity measurement occurs within a dynamic and complex organization. This means that the organization's culture, the values and experience of employees, and the political context all will have a greater impact on the measurement process. The ideal organization is the one that institutionalizes a productivity measurement system as a way of doing business.

Brinkerhoff and Dressler[5] provide the following guidelines for successful productivity and performance measurement:

- Productivity measurement must be handled as a change strategy in the organization. It requires carefully laid out groundwork and the expectation of barriers and resistance.
- Create a vision for productivity improvement through productivity measurement. Management should expect to provide strong leadership by showing a can-do attitude in the face of skepticism and barriers. The vision needs to be sold by finding win-win examples in productivity measurements improvement.
- Involve and get buy-in from senior management. Productivity efforts require massive changes in the corporate culture, policies, and procedures. These changes will need more than onetime approval of senior management.
- Aim initial efforts at targets with a high probability for success. It requires a careful survey of the organization to seek out a high potential win situation.
- Be alert to, and account for, the political ramification of measurements. The introduction of productivity measurement procedures into the current organizational context may be viewed as disruptive of the power balance. Any change in resources threatens some power bases, and offers others the opportunity for new power.
- Grow the productivity measurement effort from the ground up. This means that lower level employees should be viewed as valued partners in productivity improvement efforts. They must clearly agree that any output measurers are those that they have control over. They must be given a hunger to know how productive they are. Productivity measurement systems imposed from above are likely to involve the traditional labor argument over who is responsible for productivity.

[5] Ibid.

Build ongoing communication networks and procedures. Because productivity improvement is a process in change management, the no-surprises rule is critical. It is good to involve employees from all levels of the organization. Ongoing communication includes posting results, updating newsletters, and sending internal memos.

- Provide the necessary training and support to implement and sustain productivity improvement efforts. Analytical skills are required to look at processes and see opportunities. Productivity requires an ability to quantify and measure in simple ways. Productivity demands interpretive skills so that gathered data can be put to good use. Productivity change requires the abilities to communicate, solve problems, and coach people concerning new products and processes.

  Implementation of productivity measures requires training in basic productivity and quality concepts. Helping team leaders and supervisors conduct productivity meetings is vital to productivity improvement.

  Employees also need training in using data in decision making. People must be able to spot productivity trends. They must be able to take measurement data and determine the causes of both productivity gains and declines. Employees must be trained to use statistical process control techniques.

  Supervisors and managers need training in coaching and feedback skills. Managers who catch their subordinates in the act of doing things right will find the right behaviors repeated. Early and ongoing positive feedback can make the difference between success and failure.

- Evaluate the productivity measurement system and diffuse the process across the organization. All systems must be open for inspection and evaluation. The only effective way to evaluate productivity measurement efforts is to have clearly defined goals and benchmarks. With those in place, productivity improvement efforts can be objectively evaluated. Evaluation provides the fuel for revising productivity measurement systems. Evaluation will feed directly into finding those areas where productivity can be improved.

  Evaluation of productivity measurement results must support a reward system for those responsible for the outcome. Both public recognition and financial recognition should be in place. The culture of the organization usually prescribes the type of reward. Information about productivity progress must be made highly visible through charts and graphs of productivity growth.

  The success of the initial pilot project is very important to diffuse the process throughout the organization. Keeping internal curiosity high, but reporting the challenges and opportunities presented in the process, helps all employees, especially those who are not part of the pilot project. It is good to use personnel from the pilot as mentors or coaches in other areas of the organization. Their experience and success can be quite contagious. It also makes the system a peer-to-peer effort. Relying solely on management expertise may only slow the process of producer-level mentoring and hinder success in measuring and raising productivity.

  The traditional performance and productivity measurements, such as time schedules, on-time delivery, and cost savings, continue to be valid. However, new concepts, such as benchmarking, continuous process improvement, concurrent engineering, quality circles, self-managed teams, statistical process control, and total quality management, should be practiced and complemented with the traditional measurements.

(v) Improving Productivity

When an organization decides that improving productivity is important, there are three places to look: technological productivity, worker productivity, and managerial productivity. **Increased technological productivity** refers to the use of more efficient machines, robots, computers, and other technologies to increase outputs. **Increased worker productivity** means having workers produce more outputs in the same time period. This includes employees working harder, improving work processes, acquiring more knowledge, more resources, improved task or workplace design, and motivating employees. **Increased managerial productivity** simply means that managers do a better job of running the business. Often the real reason for productivity problems is due to poor management.

(vi) Effectiveness, Efficiency, and Economy

Effectiveness is the degree to which an organization achieves a stated goal or objective. **Efficiency** is the use of minimal resources—raw materials, money, and people—to provide a desired volume of output. **Economy** means whether an organization is acquiring the appropriate type, quality, and amount of resources at an appropriate cost.

Effectiveness and efficiency are related to productivity measurement. Effective production is the process that produces the desired results. Efficient production means achieving the desired results with a minimum of inputs. Efficiency and effectiveness must go hand in hand in productive organizations. Organizations can temporarily survive without perfect efficiency; they usually die if they are ineffective.

(h) Balanced Scorecard System

Most businesses have traditionally relied on organizational performance based almost solely on financial or accounting-based data (e.g., ROI and earnings per share) and manufacturing data (e.g., factory productivity, direct labor efficiency, and machine utilization). Unfortunately, many of these indicators are inaccurate and stress quantity over quality. They reward the wrong behavior; lack predictive power; do not capture key business changes until it is too late; reflect functions, not cross-functional processes; and give inadequate consideration to difficult-to-quantify resources, such as intellectual capital. Most measures are focused on cost, not so much on quality.

Kaplan and Norton[6] of Harvard Business School coined the term "balanced scorecard" in response to the limitations of traditional financial and accounting measures. They recommend that key performance measures should be aligned with strategies and action plans of the organization. They suggest translating the strategy into measures that uniquely communicate the vision of the organization. Setting targets for each measure provides the basis for strategy deployment, feedback, and review.

The balanced scorecard system is a comprehensive management control system that balances traditional financial measures with nonfinancial measures (e.g., customer service, internal business processes, and the organization's capacity for innovation and learning). This system helps managers focus on key performance measures and communicate them clearly throughout the organization.

[6] Robert Kaplan and David Norton, *The Strategy-Focused Organization* (Boston, MA: Harvard Business School Press, 2001).

Kaplan and Norton divided the strategy-balanced scorecard into four perspectives or categories as follows:

1. **Financial perspective.** The financial strategy focuses on matters from the perspective of the shareholder. It measures the ultimate results that the business provides to its shareholders, including profitability, revenue growth (net income), ROI, economic value added, residual income, costs, risks, and shareholder value. Financial measures are lagging measures (lag indicators); they report on outcomes, the consequences of past actions. They tell what has happened. The financial perspective is looking back.
2. **Internal business process perspective.** The internal business process focuses on strategic priorities for various business processes, which create customer and shareholder satisfaction. It focuses attention on the performance of the key internal processes that drive the business, including such measures as quality levels, efficiency, productivity, cycle time, production, and operating statistics such as order fulfillment or cost per order. Internal process measures are leading measures (lead indicators); they predict what will happen. The internal process theme reflects the organization value chain. The internal process (operations) perspective is looking from the inside out.
3. **Customer perspective.** The customer strategy is aimed at creating value and differentiation from the perspective of the customer. It focuses on customer needs and satisfaction as well as market share, including service levels, satisfaction ratings, loyalty, perception, and repeat business. The customer perspective is looking from the outside in.
4. **Innovation and learning perspective.** The innovation and learning strategy sets priorities to create a climate that supports organizational change, innovation, and growth. It directs attention to the basis of a future success—the organization's people and infrastructure. Key measures might include intellectual assets, employee satisfaction and retention, market innovation (new product introductions), employee training and skills development, R&D investment, R&D pipeline, and time to market a product or service. Innovation and learning perspective is looking ahead.

Measures should include both financial and nonfinancial. Financial measures include ROI, residual income, earnings per share, profit, cost, and sales. Nonfinancial measures include customer measures, internal business process measures, innovation and learning measures, and manufacturing measures. Customer measures include satisfaction, perception, and loyalty. Internal business process measures include efficiency, quality, and time. Innovation and learning measures include R&D investment, R&D pipeline, skills and training for employees, and time to market a product or service. Manufacturing measures include factory productivity, direct labor efficiency, and machine utilization.

A good balanced scorecard system contains both leading and lagging indicators, and both financial and nonfinancial measures. For example, customer survey (performance drivers) about recent transactions might be a leading indicator for customer retention (a lagging indicator); employee satisfaction might be a leading indicator for employee turnover (a lagging indicator), and so on. These measures and indicators should also establish cause-and-effect relationships across the four perspectives. The cause-and-effect linkages describe the path by which improvements in the capabilities of intangible assets (people) get translated into tangible customer satisfaction and financial outcomes.

The balanced scorecard provides graphical representation on strategy maps and provides a logical and comprehensive way to describe strategy. It communicates clearly the organization's desired outcomes and describes how these outcomes can be achieved. Both business units and

their employees will understand the strategy and identify how they can contribute by becoming aligned to the strategy.

WHICH SCORECARD PERSPECTIVE IS WHICH?

- The financial perspective looks back.
- The internal process perspective looks from inside out.
- The customer perspective looks from outside in.
- The innovation and learning perspective looks ahead.

(i) Production Process Flows

Three operational process flow measures include flow time, inventory, and throughput. They are interrelated in that defining targets on any two of them defines a target for the third.[7]

$$\text{Inventory} = \text{Throughput} \times \text{Flow time}$$

The basic managerial levers for process improvement are listed next.

- Decrease in flow time
- Increase in throughput
- Decrease in inventory and waiting time
- Control process variability
- Manage process flows and costs

(A) Levers for managing (decreasing) the flow time These include decreasing the work content of a critical path by shortening the length of every critical path, as shown next:

1. Reduce the work content of an activity on the critical path:
   - Eliminate non-value-adding aspects of the activity (i.e., work smarter).
   - Increase the speed at which the activity is done (i.e., work faster) by acquiring faster equipment and/or by increasing incentives to work faster.
   - Reduce the number of repeat activities (i.e., do it right the first time).
2. Work in parallel by moving some of the work content off the critical path:
   - Move work from a critical path to a noncritical path (i.e., perform work in parallel rather than in sequence).
   - Move work from a critical path to the outer loop (i.e., either preprocessing or postprocessing).
3. Modify the product mix:
   - Change the product mix to produce products with smaller work content with respect to the specified activity

[7] Ravi Anupindi, Sunil Chopra, Sudhakar D. Deshmukh, Jan Van Mieghem, and Eiten Zemel; *Managing Business Process Flows,* 2nd ed. (Upper Saddle River, NJ: Pearson/Prentice Hall, 2006), pp. 313–315.

(B) Levers for managing (increasing) throughput of a process

1. Decrease resource idleness by synchronizing flows within the process to reduce starvation and setting appropriate size of buffers to reduce blockage.
2. Increase the net availability of resources to increase effective capacity by:
   - Improving maintenance policies.
   - Performing preventive maintenance outside periods of scheduled availability.
   - Instituting effective problem-solving measures that reduce frequency and duration of breakdowns.
   - Instituting motivational programs and incentives to reduce employee absenteeism and increasing employee morale.
3. Reduce setup waste by reducing the frequency of setups and by reducing the time required for a single setup.
4. Increase the theoretical capacity by:
   - Decreasing unit load on the bottleneck resource pool (e.g., work faster, work smarter, do it right the first time, change production mix, subcontract or outsource, and invest in flexible resources).
   - Increasing the load batch of resources in the bottleneck resource pool (i.e., increase the scale of resource).
   - Increasing the number of units in the bottleneck resource pool (i.e., increase scale of process).
   - Increasing the scheduled availability of the bottleneck resource pool (i.e., work longer).
   - Modifying the production mix.

(C) Levers for reducing inventory and waiting time

1. Reduce cycle inventory (i.e., reduce batch size) by reducing setup or order cost per batch or by reducing forward buying.
2. Reduce safety inventory by:
   - Reducing demand variability through improved forecasting.
   - Reducing the replenishment lead time and its variability.
   - Pooling safety inventory for multiple locations or products through either physical or virtual centralization of specialization or some combination thereof.
   - Exploiting product substitution.
   - Using common components.
   - Postponing the product differentiation closer to the point of demand.
3. Manage safety capacity by:
   - Increasing safety capacity.
   - Decreasing variability in arrivals and service patterns.
   - Pooling available safety capacity.
4. Synchronize flows by:
   - Managing capacity to synchronize with demand.

- Managing demand to synchronize with available capacity.
- Synchronizing flows within the process.

5. Manage the psychological perception of the customers to reduce the cost of waiting.

(D) Levers for controlling process variability

1. Measure, prioritize, and analyze variability in key performance measures over time.
2. Feedback control to limit abnormal variability by:
   - Setting control limits of acceptable variability in key performance measures.
   - Monitoring actual performance and correcting any abnormal variability.
3. Decrease normal process variability by designing for processing (i.e., simplify, standardize, and mistake-proof)
4. Immunize product performance to process variability through robust design.

(E) Levers for managing process flows and costs

1. Manage flows in a plant through:
   - Process structure with cellular layout.
   - Information and material flow using demand pull system.
   - Level production with batch size reduction.
   - Quality at source with defect prevention and decentralized control.
   - Supplier management with partnerships and incentives.
   - Supply consistency through maintenance of safety capacity.
   - Employee involvement and empowerment.
2. Manage flows in a supply chain by:
   - Reducing information and material flow times using technology and efficient logistics.
   - Reducing fixed costs of ordering and quantity discounts.
   - Sharing information on customer demand and product availability.
   - Coordinating forecasts between affected parties.
   - Stabilizing prices.
3. Improve processes through:
   - Continuous improvement and reengineering.
   - Increased visibility; incentives; plan-do-check-act (PDCA) cycle; and benchmarking.

3.5 Inventory Management Techniques and Concepts

From inventory management viewpoint, demand is of two types: independent demand and dependent demand. Independent demand inventory systems are based on the premise that the demand or usage of a particular item is independent of the demand or usage of other items. Examples include finished goods; spare parts; material, repair, and operating supplies; and resale inventories.

(a) Independent Demand Inventory Systems

Independent demand inventory systems are "pull" systems in that materials are pulled from the previous operation as they are needed to replace materials that have been used. An example: Finished goods are replaced as they are sold. These types of inventory systems answer the question of when to place the replenishment order and how much to order at one time. Reorder point models and fixed/variable order quantity models (e.g., economic order quantity [EOQ]) are examples of independent demand inventory systems as they do review inventory either continuously or periodically. Four possibilities exist:

1. Continuous review and fixed order quantity
2. Periodic review and fixed order quantity
3. Continuous review and variable order quantity
4. Periodic review and variable order quantity

(b) Dependent Demand Inventory Systems

Dependent demand inventory systems are based on the premise that the demand or usage of a particular item is dependent on the demand or usage of other items. Examples include raw materials, work-in-process inventories, and component parts.

(c) Inventory Levels and Investment Levels

A company manages its inventory by using various methods and approaches (e.g., EOQ). Inventory consists of raw materials, work in process (WIP), and finished goods. Efficient inventory management is needed to support sales, which is necessary for profits. Benefits such as high turnover rate, low write-offs, and low lost sales can be attributed to efficient inventory management. These benefits, in turn, contribute to a high profit margin, a higher total asset turnover, a higher rate of ROI, and a strong stock price. Inventory management is a major concern for product-based organizations (e.g., manufacturing, retail), since 20% to 40% of their total assets is inventory. As such, poor inventory control will hurt the profitability of the organization.

KEY CONCEPTS TO REMEMBER: Inventory Management

- The larger the amount of inventories held, the longer the inventory conversion period, hence the longer the cash conversion cycle.
- The smaller the amount of inventories held, the shorter the inventory conversion period, hence the shorter the cash conversion cycle.
- A shorter cash conversion cycle is preferred over a longer cash conversion cycle.
- Errors in establishing inventory levels can lead to lost sales, lost profits, or increased costs.
- A lower investment in inventories will increase the rate of ROI, and the value of the firm's stock increases.
- Too much reduced investment in inventories could lead to lost sales due to stock-outs or to costly production slowdowns.

Inventory levels and account receivables levels directly depend on sales levels. Receivables arise after sales have been made while inventory must be acquired or produced ahead of sales. Inventory managers have the responsibility to maintain inventories at levels that balance the benefits of reducing the level of investment against the costs associated with lowering inventories. A company's inventory is related to the amount of expected sales. The company's financial forecasting of inventory in the following year would be most accurate when applying simple linear regression method.

(d) Efficient Inventory Management

Efficient inventory management focuses on three areas: investment in inventory, optimal order quantity, and reorder point (see Exhibit 3.30).

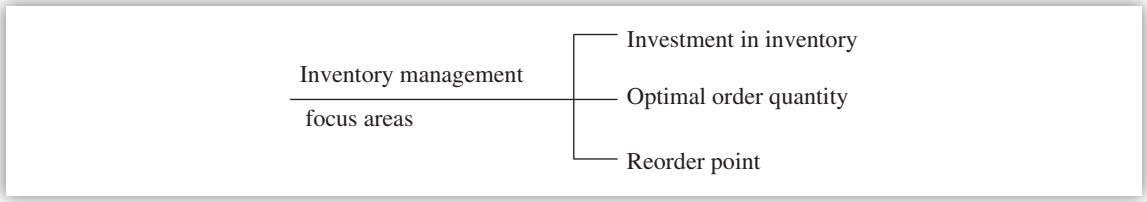


EXHIBIT 3.30 Inventory Management Focus Areas

(e) Investment in Inventory

Investment in inventory depends on the actual level of inventory carried. The relevant question is how many units of each inventory item the firm should hold in its stock. Two types of stock concepts must be understood: working stock and safety stock. The actual level of inventories carried will equal the sum of the working stocks and safety stocks.

A **working stock** is needed to meet normal, expected production and sales demand levels. Producing more goods than are currently needed increases the firm's carrying costs and exposes it to the risk of obsolescence if demand should fall. Remember that demand for sales is uncertain. EOQ establishes the working stock amount. EOQ is discussed later in this section.

A **safety stock** is needed to guard against changes in sales rates or delays in production and shipping activities. Safety stock is additional stock beyond the working stock and satisfies when demand is greater than expected. The additional costs of holding the safety stock must be balanced against the costs of sales lost due to inventory shortages. Safety stock will not affect the reorder quantities.

KEY CONCEPTS TO REMEMBER: Safety Stock

- The optimum safety stock increases with the uncertainty of sales forecasts, lost sales resulting from inventory shortages, and probability of delays in receiving shipment.
- The optimum safety stock decreases as the cost of carrying it increases.

Effective management requires close coordination and communication among the various functional departments of the organization, such as the marketing, sales, production, purchasing,

and finance departments. Sales plans need to be converted into purchasing and production plans producing finished goods and for acquiring raw materials; financing plans are needed to support the inventory buildup.

Since inventories need to be available prior to sales, an increase in production to meet increased sales requires an increase in notes payable (a liability account). Since assets (inventories) are increasing, liability (notes payable) must also increase.

Investment in inventory is not complete without discussing the various costs associated with inventories due to their direct relationships. The cost structure affects the amount and type of investment needed. Three types of inventory-related costs are: carrying costs, ordering costs, and (3) stock-out costs, as shown in Exhibit 3.31.

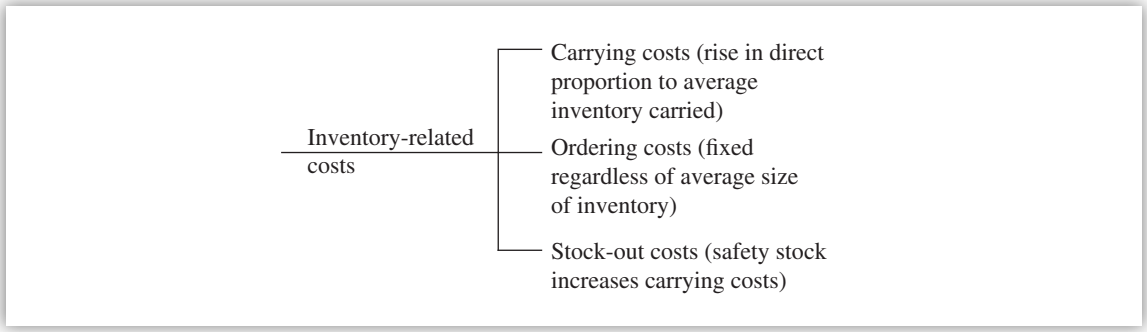


EXHIBIT 3.31 Inventory-Related Costs

(i) Carrying Costs

The costs associated with carrying inventories, including storage, capital, and depreciation costs are known as carrying costs. Carrying costs rise in direct proportion to the average amount of inventory carried which, in turn, depends on the frequency with which orders are placed. That is, an increase in the frequency of inventory ordering will reduce total carrying costs.

$$\text{Annual total carrying costs} = (C)\ (P)\ (A)$$

where C = Percentage cost of carrying inventory—that is, (Capital cost + Storage cost + Insurance + Depreciation and obsolescence cost + Property taxes) ÷ Average inventory value
P = Percentage price per unit
A = Average number of units—that is (Annual sales ÷ Number of orders) ÷ 2 (P).
= Average inventory value

(ii) Ordering Costs

The cost of placing and receiving an order is known as the ordering costs, which is fixed regardless of the average size of inventories.

$$\text{Total ordering costs} = (F)\ (N) = (F)\ (S \div Q)$$

where F = Fixed costs associated with ordering inventories
N = Number of orders per year
S = Sales in units
Q = Quantity ordered in units

$$\text{Total inventory cost} = \text{Total carrying cost} + \text{Total ordering cost}$$

(iii) Stock-out Costs

Safety stock reduces stock-out costs. The safety stock is useful in protecting against delays in receiving orders. However, safety stock has a cost. The increase in average inventory resulting from the safety stock causes an increase in inventory carrying costs.

CARRYING COSTS VERSUS ORDERING COSTS VERSUS STOCK-OUT COSTS

- The components of **carrying costs**, which increase in proportion to the average amount of inventory held, include the costs of capital tied up in inventory, storage, and handling costs, insurance premiums, property taxes, depreciation, and obsolescence cost.
- The components of **ordering costs**, which are fixed regardless of the average size of inventories, include the cost of placing orders including production setup and shipping and handling costs.
- The components of **stock-out costs**, which are costs of running short, include the loss of sales, the loss of customer goodwill, and problems or delays in production schedules.

(f) Optimal Order Quantity

How many units should be ordered or produced at a given time is a major question faced by the inventory manager. Either too much or too little inventory is not good. An optimum inventory level is designed and is found through the use of the EOQ model. EOQ provides the optimal, or least-cost, quantity of inventory that should be ordered.

If a company's cost of ordering per order increases while carrying costs per order remain the same, the optimal order size as specified by the EOQ model would increase.

EOQ COST CHARACTERISTICS

- The point at which the total cost curve is minimized represents the EOQ, and this, in turn, determines the optimal average inventory level. Here, total cost is the sum of ordering and carrying costs.
- Some costs rise with larger inventories whereas other costs decline.
- The average investment in inventories depends on how frequently orders are placed.
- Ordering costs decline with larger orders and inventories due to reduced order frequency.

If Q is the order quantity, then the how-much-to-order decision involves finding the value of Q that will minimize the sum of holding and ordering costs.

$$Q = \text{EOQ} = \sqrt{\frac{2D\ Co}{Ch}}$$

where D = Annual sales demand in units
Co = Cost of placing one order
Ch = Cost of holding (or carrying) one unit in inventory for the year

Note that the data needed to calculate EOQ includes the volume of product sales, the purchase price of the products, the fixed cost of ordering products, and carrying costs. It does not include

the volume of products in inventory, inventory delivery times, delays in transportation, or quality of materials.

Due to the square root sign, a given increase in sales will result in a less-than-proportionate increase in inventories, and the inventory turnover ratio will increase as sales grow.

(g) Reorder Point

Another major problem facing the inventory manager is at what point inventory should be ordered or produced. The point at which stock on hand must be replenished is called reorder point. It is also the inventory level at which an order should be placed. The formula is

$$\text{Reorder point} = \text{Lead time} \times \text{Usage rate}$$

where Lead time = Time lag required for production and shipping of inventory
Usage rate = Usage quantity per unit of time (Note: The time period should be the same in both lead time and usage rate—that is, days, weeks, or months.)

A complication in the calculation of the reorder point arises when we introduce a concept of goods in transit. This situation occurs when a new order must be placed before the previous order is received. The formula for a reorder point when goods-in-transit is considered is

$$\text{Reorder point} = (\text{Lead time} \times \text{Usage rate}) - (\text{Goods in transit})$$

KEY CONCEPTS TO REMEMBER: Reorder Point

- Goods in transit are goods that have been ordered but have not been received.
- A goods-in-transit situation exists if the normal delivery lead time is longer than the time between orders.

(h) Inventory Decisions

Inventory managers face two decision rules in the management of inventories: "how much to order" and "when to order" that will result in the lowest possible total inventory cost. The how-much-to-order decision rule can be satisfied with the use of an EOQ. This decision rule involves selecting an order quantity that draws a compromise between (1) keeping smaller inventories and ordering frequently (results in high ordering costs) and (2) keeping large inventories and ordering infrequently (results in high holding costs). The when-to-order decision rule can be satisfied with the use of a reorder point.

ORDERING COST VERSUS HOLDING COST

- Ordering costs are the costs associated with placing an order and include salaries of the purchasers, paper, postage, telephone, transportation, and receiving costs.
- Holding costs are the costs associated with carrying a given level of inventory; these costs are dependent on the size of the inventory. They include interest cost for the capital tied up in inventory, opportunity cost associated with not being able to use the money for investment, insurance fees, taxes, pilferage, and damage, as well as other warehouse overhead costs.

(i) Calculating How Much to Order

The focus of EOQ method is on the quantity of goods to order that will minimize the total cost of ordering and holding (storing) goods. EOQ is a decision model that focuses on the trade-off between carrying costs and ordering costs. It calculates the order quantity that minimizes total inventory costs. Calculus is used in determining the EOQ.

EOQ is appropriate for managing the finished goods inventories, which have independent demands from customers or from forecasts. The holding cost, the ordering cost, and the demand information are the three data items that must be prepared prior to the use of the EOQ model. If Q is the order quantity, then the how-much-to-order decision involves finding the value of Q that will minimize the sum of holding and ordering costs.

$$Q = \text{EOQ} = \sqrt{\frac{2D\ Co}{Ch}}$$

where D = Annual demand
Co = Cost of placing one order
Ch = Cost of holding one unit in inventory for the year

Annual inventory holding cost is directly related to the amount of inventory carried. The EOQ will rise following an increase in the fixed costs of placing and receiving an order.

Exhibit 3.32 describes costs for inventory. Line (A) represents annual total cost, Line (B) represents total annual inventory holding costs, Line (C) represents the minimum-total-cost order quantity, and Line (D) represents total annual ordering cost.

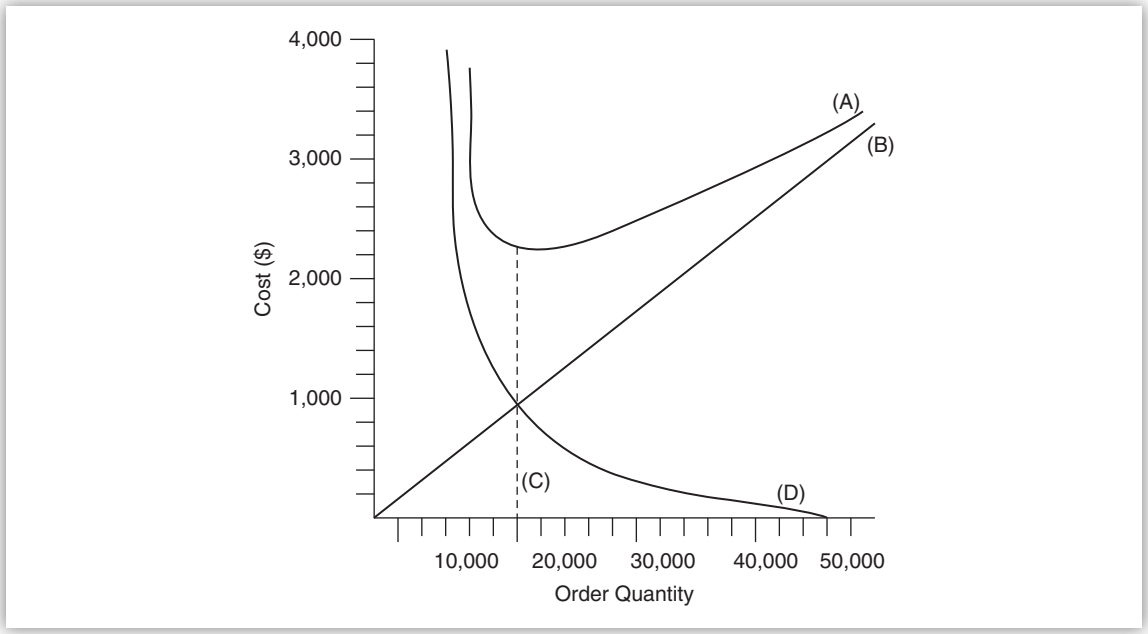


EXHIBIT 3.32 Cost for Inventory

CALCULATION OF OPTIMUM ORDER SIZE

A firm expects to sell 1,000 units of product X during the coming year. Ordering costs are $100 per order, and carrying costs (holding costs) are $2 per unit per year.

Question: Using the EOQ model, what is the optimum order size?

Answer: The optimum order size is 317, as shown next.

The answer is to find the square root of (2 × $100 × 1,000) ÷ $2. This is the square root of 100,000, or 317.

(j) EOQ Assumptions

Two major assumptions of EOQ are discussed next.

1. **The demand for an item is constant.** Since the constant demand assumption is not realistic, managers would have to be satisfied with the near-minimum-cost order quantity instead of a minimum-total-cost order quantity.
2. **The entire quantity ordered arrives at one point in time.** Again, this may not be realistic because some vendors will deliver partial shipments. Managers usually add a judgmental value-based order quantity to the EOQ suggested order quantity to accommodate unrealistic assumptions of constant demand rate by the EOQ model.

Specific assumptions of the EOQ model include:

- Sales can be forecasted perfectly. This is unrealistic.
- Sales are evenly distributed throughout the year. This is not real. What about seasonal or cyclical demands?
- Orders are received without delay. This is also unrealistic.
- Fixed costs, carrying costs, and purchase prices are all fixed and independent of the ordering procedures. This is not possible either.

CONTROLS IN MATERIAL REQUIREMENT CYCLE

EOQ models, ABC inventory analysis, just-in-time (JIT), and kanban systems are commonly used controls in material requirements cycle.

(k) Sensitivity Analysis and EOQ

It is good to know how much the recommended order quantity would change if the estimated ordering and holding costs had been different. Depending on whether the total annual cost increased, decreased, or remains the same, we can tell whether the EOQ model is sensitive or insensitive to variations in the cost estimates.

(l) Calculating When to Order

The when-to-order decision rule is expressed in terms of a reorder point as follows:

$$r = d \times m$$

where r = Reorder point
d = Demand per day
m = Lead time for a new order in days

The cycle time answers how frequently the order will be placed, and it can be calculated as:

Cycle time = Number of working days in a year ÷ Number of orders that will be placed in a year

(m) Safety Stock and Stock-outs

Safety stock is the amount of extra stock that is kept to protect against stock-outs. Running out of an inventory item is called a stock-out situation. Safety stock is the inventory level at the time of reordering minus the expected usage while the new goods are in transit.

The goal is to minimize both the cost of holding a safety stock and the cost of stock-outs. EOQ is not relevant to stock-outs. Production bottlenecks leads to a stock-out. Factors to be considered in controlling stock-outs include time needed for delivery, rate of inventory usage, and safety stock.

(n) ABC Inventory Control System

ABC is a method of classifying inventory based on usage and value. Expensive, frequently used, high stock-out cost items with long lead times are most frequently reviewed in an ABC inventory control system. Inexpensive and infrequently used items are reviewed less frequently.

APPLICATION OF ABC INVENTORY SYSTEM

A firm uses an ABC inventory control system. About 10% of inventory items are classified into group A. Another 20% are in group B. The remainder is in group C. Which classification is most likely to hold the greatest number of days of supply?

a. Group C
b. Group B
c. Group A
d. All groups are likely to have an equal number of days of supply

Answer **a** is correct. Group C items are low-dollar-value items and receive less management attention. Extensive use of models and records is not cost effective. It is cheaper to order large quantities infrequently. Group A items are high-dollar value, and management would try to keep investment in such items low. Therefore, by definition, choices b, c, and d are incorrect.

(o) Effects of Inflation on Inventory Management

There is no evidence that inflation either raises or lowers the optimal level of inventory of firms in the aggregate. It should be considered since it will raise the individual firm's optimal inventory holdings if the rate of inflation is above average, and vice versa.

Decision rules and consequences of inflation are listed next.

- For a moderate inflation, it is safe to ignore inflation and the benefit is not worth the effort.

- For a relatively constant inflation, subtract the expected annual rate of inflation from the carrying cost percentage (C) in the EOQ model and recalculate the EOQ. Since the carrying cost will be smaller, the recalculated EOQ and the average inventory will increase.
- For higher inflation, the higher the rate of inflation, the higher the interest rates will be, and this will cause carrying cost to increase and thus lower the EOQ and average inventories.

(p) Just-in-Time Systems

(i) JIT Strategy

JIT is a production strategy to continuously improve productivity and quality. It is based on the belief that small could be better, not "more" is better. An effective JIT strategy encompasses the entire product life cycle from the acquisition of raw materials to delivery of the end product to the final customer. *The scope includes topics such as JIT purchasing, processing, inventory, and transportation.* Each topic is discussed next.

JIT is based on these management principles:

- Eliminate waste.
- Produce to demand and one at a time.
- Think long term.
- Develop, motivate, trust, and respect people.
- Achieve continuous improvement

JIT is made possible when the focus is quality at the source, and the tools used are statistical process control methods, fail-safe methods, and problem-solving methods. **Quality at the source** means producing perfect parts every time and all the time. The major benefits of JIT strategy are improved productivity, quality, service, and flexibility; and reduced costs, inventory investment, lead times, lot sizes, and physical space.

(ii) JIT Purchasing

JIT purchasing requires a partnership between a supplier and a customer, which is a major departure from the traditional purchasing. JIT supplier relations call for long-term partnerships with single-source suppliers that provide certified quality materials while continuously reducing costs. The JIT supplier's manufacturing processes must be under statistical process control, and its capability should be certified by the customer. The statistical process control charts serve as the documentation to ensure that the process stayed in control during the time the parts were made.

JUST-IN-TIME PURCHASING

Under JIT purchasing, competitive bidding may not occur prior to selecting a supplier because of sole-sourcing, single-sourcing, or dual-sourcing approaches taken. The supplier is selected based on quality, commitment to excellence, and performance, not cost.

A JIT supplier is expected to support the production flow with frequent, small-lot shipments that can be used immediately by the customer. Usually, no inspection is required at the receiving side of the materials.

A JIT supplier will have to become a JIT producer with the idea of pushing costs out of the supply chain, not to pass costs down to the next supplier. Since the JIT supplier is considered as a partner, the customer must notify the supplier of plant disruptions, temporary shutdowns, or anticipated engineering changes so that the supplier can make adjustments to production schedules and inventory plans. Doing this requires sharing of information and open communications.

TRADITIONAL PURCHASING PRACTICES VERSUS JIT PURCHASING PRACTICES

- Traditional purchasing practices call for infrequent, large-lot shipments.
- JIT purchasing practices call for frequent, small-lot shipments.
- Traditional purchasing practices call for inspection, since they focus on continuous checking by the customer. These practices are reactive due to their focus on "after the fact."
- JIT purchasing practices call for no inspection, since they focus on continuous improvement by the supplier. JIT is proactive due to its focus on "before the fact."

(iii) JIT Production Processing

JIT production processing requires setup reduction, focused factory, group technology, uniform scheduling and mixed model scheduling, and the pull system. The objective here is to produce many varieties of products in small quantities on short notice. Manufacturing flexibility is the hallmark of the JIT production processing strategy.

(A) Setup Reduction Traditional production systems require large lot sizes due to excessive setup or changeover time. JIT suggests reduced setup time so that lot sizes are reduced or evolve to lot size of 1 with the first piece made good every time. The goal is to accomplish any setup in single minutes (i.e., in less than 10 minutes). Setup reduction requires eliminating equipment downtime and machine adjustments as much as possible combined with good housekeeping in the manufacturing plant.

With reduction in setup time comes many other benefits, such as:

- Increased quality due to closer tie-in between the machine operator and the setup.
- Increased productivity and profitability due to elimination of many non-value-added activities associated with moving, storing, inspecting, and reworking.
- Reduced manufacturing lead time resulting in lower inventories and associated physical space requirements.
- Reduced scrap, lowering unit costs.

(B) Focused Factory **Focused factory** is a concept where the plant layout is dedicated to a single product family that maximizes overall productivity and quality while minimizing space and resource requirements. It is intended to physically link all the involved manufacturing operations together to minimize the distance between them, minimize the complexity, maximize the integration of tasks, and enhance the interaction between the workers. This approach eliminates waste and increases communications.

(C) Group Technology While focused factory is a macro approach, group technology is a micro approach in which equipment is laid out to produce a family of parts, one at a time, by physically

linking all possible operations in the process. It can be viewed as self-contained, integrated parts factories within the focused factory.

Group technology uses a cell concept where the shape of the cell is a U or C so the starting and ending points are near each other to save walking time. The idea is that a single worker performs every operation, in the proper sequence, to make one finished unit at a time. All operations are close together as much as possible with little or no staging space between workstations. A worker in a group technology cell not only performs every operation in the process but also sees how they relate to one another. This improves productivity and quality.

GROUP TECHNOLOGY VERSUS TRADITIONAL TECHNOLOGY

- Group technology is a low-volume, high-mix work center for an entire family of similar parts.
- Traditional technology is a high-volume, single-part work center.

(D) Uniform and Mixed Model Scheduling Uniform scheduling calls for smaller lot sizes, eventually making every part every day. It is a variable flow management concept instead of trying to coordinate "lumps" of production. It provides level loading for manufacturing operations, building the same product mix every day during a given month. Levels may change from month to month, and hence the term "variable" flow. Under uniform scheduling, the interval between like units is called cycle time. The shorter the cycle time, the faster the parts will be made.

Mixed model scheduling is employed to produce the same parts every hour. Yet production levels will change from month to month to meet customer demand.

(E) Pull System Conventional scheduling systems pushes orders through the production shop, making it difficult to synchronize the diverse activities required to produce the end products. This method results either in excess inventory or in insufficient inventory.

Like uniform scheduling, the pull system is based on the variable flow manufacturing principle to make parts repetitively in a low-volume production. The pull system links every process in the plant using simple signaling cards to synchronize production with changing customer demands. It uses a production signal to authorize the machine center to produce parts that have been taken from the storage area next to it. It uses a withdrawal signal as a permission to consume.

PUSH SYSTEM VERSUS PULL SYSTEM

- The push system is based on a fixed-flow manufacturing principle.
- The pull system is based on a variable-flow manufacturing principle.
- The traditional (push) production system has a "contingency" (i.e., safety stock) mentality.
- The JIT (pull) production system has "no contingencies" (i.e., no safety stock) mentality.

The pull system uses standard lot sizes and employs standard-size containers to enhance visual control on the factory floor. This sets the stage for a "precision" mentality. The pull system

ensures that the right parts will be in the right place at the right time with a minimal investment in inventory. The pull system provides better production control for less cost.

(iv) JIT Inventory

A misconception about JIT is that it is just a program to reduce inventory. Fortunately, JIT does more than that. JIT purchasing is called "stockless inventory"; the customer has no inventory to stock as it is used up in the production right after it was received. The major goal is to reduce or eliminate work-in-process inventory so that all raw materials are consumed in the production process.

(v) JIT Transportation

While JIT purchasing is the starting point of a JIT cycle, JIT transportation is the execution part of the JIT cycle. JIT transportation is the physical linkage between the inside and the outside processes. It is a process that starts at a supplier location and ends at a customer location. It requires the analysis of all transport events and elimination of the non-value-added events. The basic value-added events include:

1. Move load to dock at a supplier location.
2. Load carrier.
3. Move load to customer location.
4. Return empty trailer to terminal.
5. Unload by the customer.
6. Move load to assigned customer location.

Similar to JIT supplier–customer partnership, JIT transportation requires that all three parties—supplier, carrier, and customer—work together more closely than ever before. With frequent, small quantities moved each time, the traffic at both the supplier and the customer plants will increase, creating a demand for rapid load and unload capabilities.

To support JIT flow of production, frequent, time-of-day deliveries will be required. This means receiving parts at a specific customer location on specific days at specific times during those days.

Reusable containers and small delivery windows are new approaches. Reusable containers save money when compared with expendable containers. Small delivery windows means rapid loading and unloading, which can be enhanced by using point-of-use doors, driver self-unloading, and innovative equipment, such as portable ramps and end-loading trailers.

(q) Materials Requirements Planning

Materials requirements planning (MRP) is suitable for managing raw materials, components, and subassemblies, which have dependent demands that may be calculated from the forecasts and scheduled production of finished goods. In other words, the order for component inventory is placed based on the demand and production needs of other items that use these components.

Benefits of MRP include reduced investment in inventory, improved workflow, reduced shortage of raw materials and components, and reliable delivery schedules.

DETERMINISTIC INVENTORY VERSUS PROBABILISTIC INVENTORY

- Deterministic inventory models assume that the rate of demand for the item is constant (e.g., EOQ).
- Probabilistic inventory models assume that the rate of demand for the item fluctuates and can be described only in probability terms.

In addition to considering dependent demand in the determination of net requirements for components, an MRP system also determines when the net requirements are needed by using the time-phasing concept. This concept works by starting with the time that the finished product must be completed and working backward to determine when an order for each component must be placed based on lead times.

The approach to determining net requirements whenever a dependent demand situation exists is:

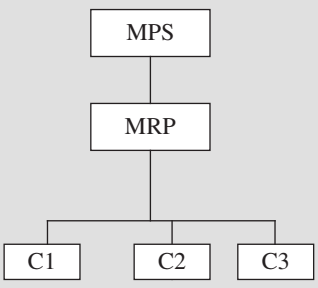
$$\text{Net component requirement} = \text{Gross component requirement} - \text{Scheduled receipts} - \text{Number of components in inventory}$$

where Gross component requirement = Quantity of the component needed to support production at the next higher level of assembly

EOQ VERSUS MRP

- The EOQ model focuses on finished goods inventories, which have an independent demand from customers or from forecasts.
- The demand for raw materials and components in the MRP model is directly dependent on the demand for the finished goods in the inventory system.

MRP systems are used to project inventory stock levels because they depend on the amount and timing of finished goods to be produced and then determine the requirements for raw materials, parts, components, and subassemblies at each of the prior stages of finished goods production. Working backward, each end product is sequentially exploded or separated into its necessary components and raw materials (i.e., to project inventory stock levels needed). MRP can also be used to do resource planning (capacity planning and labor scheduling) and materials planning. The relationship among the MRP system, the master production schedule (MPS) system, and a bill of materials (BOM) is shown in Exhibit A.



- MPS indicates units of finished goods to be produced each time period.
- BOM defines the components required by each finished product. MRP uses the BOM to determine the number of components (C1, C2, C3,...C*n*) required.
- Shows forecasted quantity for each component with dates.

EXHIBIT A Relationship among MRP, MPS, and BOM

The inputs to MPS are forecast orders and actual orders. The inputs to MRP are MPS data, BOM data, and the current inventory file. The outputs from the MRP system are the requirements for each item in the BOM along with the dates each item is needed, which, in turn, is used to plan order releases for production and purchasing.

The BOM is a structured parts (components) list showing the hierarchical relationship between the finished product and its various components. The BOM indicates exactly how many components are needed to produce the quantity of finished goods recommended by the MPS system.

MRP is a computer-based application system and an example of the dependent demand inventory system. It is a system to determine quantity and timing requirements of materials used in a manufacturing operation. Materials can be purchased externally or produced in-house. MRP utilizes a master production schedule, a product BOM, and current inventory data to determine current new requirements and timing of materials.

The **objectives** of the MRP system are to determine what, how much, and when to order and also when to schedule deliveries and to keep priorities current for inventory planning, capacity requirements planning, and shop floor control.

The **benefits** of an MRP system come from doing a better job of managing the planning process. Specifically, benefits include lower inventories, better scheduling, early warning system about capacity and supply problems, and long-range plans in terms of equipment and labor needs.

The **prerequisites** for a successful implementation of an MRP system include a feasible master production schedule, accurate inventory records, accurate BOM, known lead times, and unique part numbers.

A master production schedule is *feasible* if the resulting production schedule is practical in terms of material availability, labor capacity, and machine capacity. The planning horizon for the master production schedule should be at least equal to the longest cumulative procurement and manufacturing lead time for an end item. The master production schedule is based on confirmed customer orders, interplant orders, forecast sales, and current inventory levels. The result is a plan of end items production that translates into the needs for all subassemblies, component parts, and raw materials.

Accurate inventory records are necessary to determine the appropriate quantity and timing of each item to order or manufacture. Cycle counting is generally used to maintain the required inventory accuracy.

Accurate BOM tells the MRP system what items are used to produce the finished product or subassembly and in what quantity. A variety of display formats exists for BOM, including the single-level BOM, indented BOM, modular (planning) BOM, transient BOM, matrix BOM, and costed BOM. The BOM may also be called the formula, recipe, or ingredient list in certain process industries.

The MRP system requires a lead-time estimate for every part number in the system. This is called **known lead times**. Incorrect lead-time information leads to incorrect purchasing decisions. It is

essential that lead times be updated promptly for all internally produced or externally supplied parts and raw materials.

The MRP system requires that each part be identified with a **unique part number** no matter where it is used in the company. Duplicate part numbers and incorrect part numbers are common problems.

(r) Distribution Systems

Inventory in a distribution system can be managed through the use of independent demand models such as continuous and periodic review models. Examples of these models include single order point, double order point, periodic review system, and sales replacement system, which are described below.

The primary **advantage** of the distribution models is that they allow the various levels in the distribution chain to manage their inventories autonomously. The primary **disadvantage** of these models is that they ignore the other stages in the supply chain, leading to stock-outs and back orders. Excess shipping costs can be incurred since no one is coordinating the movement of materials within the system. Also, the demand for replenishment occurs without any regard for what is currently being produced or planned to be produced. Under these situations, the need for an item incurs extra setup costs, lost productivity, and excess transportation costs.

(i) Single Order-Point System

The single order-point system basically ignores the fact that the order takes place in a chain and assumes that each element in the distribution system is independent of all other components. This independent behavior can cause large swings caused by a phenomenon called "lumpy demand" at the next level down in the distribution chain. The lumpy demand comes from the lack of communication and coordination among the factory, warehouse(s), distributors, and retailers.

(ii) Double Order-Point System

The double order-point system considers two levels down in the distribution system, hence the name "double." For example, if a distributor is quoted a lead time from the factory warehouse of two weeks and it takes the factory warehouse three weeks to have stock replenished, the reorder point is set based on the demand for a five-week period. It does not produce lumpy demand, as does the single order point system. An advantage is that it reduces the risk of stock-outs. Increasing the safety stock is its disadvantage.

(iii) Periodic Review System

In a periodic review system, orders are placed on a predetermined time schedule. The advantage is that the order times can be staggered throughout the chain to smooth the demand at each point in the distribution chain. This reduces peaks and valleys caused by several customers ordering at the same time.

(iv) Sales Replacement System

In the sales replacement system, the supplier ships only what the customer used or sold during the period. The objective is to maintain a stable inventory level in the system. This method requires having enough inventory to cover the potential demand during the replenishment cycle. In essence, the sales replacement system is a periodic review model with variable order quantities.

(v) Distribution Requirements Planning

Distribution requirements planning (DRP) is an application of the time-phasing logic of MRP applied to the distribution system. The purpose of DRP is to forecast the demand by distribution center to determine the master production scheduling needs. DRP uses forecasts and known order patterns from customers in the distribution chain to develop the demand on the master schedule.

DISTRIBUTION REQUIREMENT PLANNING VERSUS ORDER POINT–BASED DISTRIBUTION SYSTEM

- The DRP anticipates the future needs throughout the distribution chain and plans deliveries accordingly.
- The order point-based distribution system does not anticipate future needs. It simply reacts to the current needs.

(vi) Inventory Distribution Methods

The functions of warehouse distribution, production, and purchasing are closely interrelated and constantly interacting with each other in a manufacturing firm. The decision problems considered during inventory distribution strategy are:

- When, what, and how much of it to ship to a warehouse.
- When, what, and how much of it to produce at the factory, with what size workforce.
- When, what, and how much of it to purchase as inputs to the factory warehouse system.

(vii) Warehouse Inventory Control

Warehouses usually stand in a distribution system between a factory and final customers or other warehouses, as shown in Exhibit 3.33.

EXHIBIT 3.33 Warehouse Inventory Control

On the sales side, the warehouses face a demand from customers that usually is subject to random demand fluctuations and usually requires fast service. On the supply side, the warehouse usually faces a significant and sometimes erratic lead time for receiving shipments of products from factories.

Payments to carriers for making shipments to the warehouse are frequently of major importance in designing the warehouse ordering and distribution system. Economies usually can be achieved by increasing the size of shipment up to some upper limit, such as a full truckload or carload. Efforts to economize on shipping costs by increasing the size of shipments increase the time between shipments and hence decrease the speed of service.

(viii) Types of Warehouse Shipments

Warehouses usually stock a very large number of products—the larger the shipment size, the more products are involved, and the greater are the problems of controlling the inventories of

different products jointly. These are some of the considerations involved in decisions to order shipment to warehouses. Two basic types of shipments can take place: periodic shipments and trigger shipments (see Exhibit 3.34).

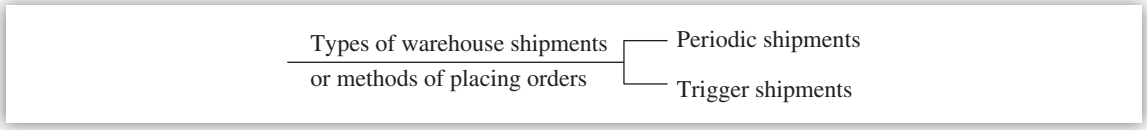


EXHIBIT 3.34 Types of Warehouse Shipments or Methods of Placing Orders

(A) Periodic Shipments The periodic system of placing orders has the virtue of automatically synchronizing the decisions on many products. Under this system of operation, warehouse shipping decisions can be handled in two steps. First, the product can be considered in the aggregate, and next the shipping costs for different sizes of shipping lot can be weighed against the cost of holding inventory associated with each size lot. On this basis, the optimum shipping lot can be determined. By using the forecasted aggregate shipping rate, the decision period can be determined.

The shipment received at the beginning of a period is associated with the period because that shipment must carry the warehouse through the period. However, because the lead time *Tl* is required to obtain the shipment, the order for the *t*th period must be initiated a length of time *Tl* before the beginning of the *t*th period. When the time arrives for placing an order, the inventory records for the products involved are brought up to date. The position of inventories on hand and on order is then known. The orders can then be placed for the amount of each product to be included in the shipment on the basis of expected product sales, initial inventory position at the time of ordering, and expected final inventory position at the end of the period.

In calculating the distribution of forecast errors, the forecast span is (*Tl* + *Td*), where *Td* is the length of the decision period, which is equal to the interval between the receipt of shipments. When decisions on the timing of a shipment are made in advance, any random fluctuations in aggregate sales tend to cause shipment sizes to vary randomly. This may be quite satisfactory in situations where shipments of less than truckload or carload are being made and variations in the size of the shipment can be accommodated readily. If the fluctuations in the size of the shipment exceed the available capacity, a supplementary shipment may be required or the aggregate inventory buffer may be changed.

(B) Trigger Shipments A warehouse may aggregate its products and decide on the optimal size of shipment but allow timing to be triggered by sales. Because the timing of shipments is irregular, orders for individual products cannot depend on a simple constant lead time. Instead, *the lead time for any single product is a random variable that depends partly on orders placed for other products.* When the total orders for all products have reached the total desired for a shipping lot, the orders will be placed for a shipment. Under this system, the lead time for any one product is a random variable that depends on the random sales of other products. The outcome for an individual product depends on the correlation between its sales and the aggregate sales.

(C) Advantages and Disadvantages This trigger system is more responsive to fluctuations in sales than the periodic system is. It has the further advantage that the shipment size is predetermined rather than random; hence problems of overburdening carrier capacity are minimized. However,

the costs of administering the continuous review of inventory position for a trigger system are usually somewhat higher than under the periodic system.

(ix) Other Warehouse Considerations

In estimating the cost of alternative shipping carriers, the cost of having valuable inventory tied up while the vehicle is in transit should be considered. While this cost usually is not large, taking it into account will systematically lower the costs of using faster rather than slower carriers. Another economy associated with fast shipments that may be overlooked is the fact that time in transit is one component of the lead time. *Shortening the lead time allows a reduction in the inventory buffers and hence a decrease in inventory holding costs.*

A warehouse may be put under a financial constraint in response to the working capital needs of the company; the warehouse also may be constrained by the production-smoothing requirements of the factory, and the warehouse itself may have certain constraints on its capacity to receive shipment or its storage space. Some constraints may be equality constraints on the exact amount of inventory that should be held, and some may be inequality restraints that establish upper or lower limits. Briefly stated, if an inequality restraint is not violated when the corresponding variable is set to zero, then the constraint can be ignored. If it is violated, then the solution is carried through as if an exact constraint applied.

In estimating the costs of stock-outs at the warehouse, the least costly alternative should be used. If the warehouse is out of stock on a product, it may disappoint a customer, or it may initiate a rush order from another warehouse or from the factory. In the latter cases, the cost of depletion may well be the cost of making a special rush shipment, taking into account the communication and expediting costs. Although few warehouses keep adequate records on stock-outs and failures to render customer service, these data could be useful in estimating depletion costs as well as costs associated with customer service.

When estimating the cost of holding inventory, the cost of obsolescence should be considered. The indirect costs of having very large inventories in a warehouse may be increased because of product damage resulting from high stacking. Also, increased handling costs from crowded aisles and poor housekeeping and access may show up as overtime payments.

A single warehouse may utilize several different decision systems on different types of products, or products from different suppliers according to particular needs. For example, fast-moving products might be segregated from slow-moving products, and a different decision system may be used for each.

(s) Production Scheduling and Control Systems

Four types of production scheduling and control systems will be discussed in this section. These include: JIT systems, traditional systems, kanban systems, and bar coding systems (see Exhibit 3.35).

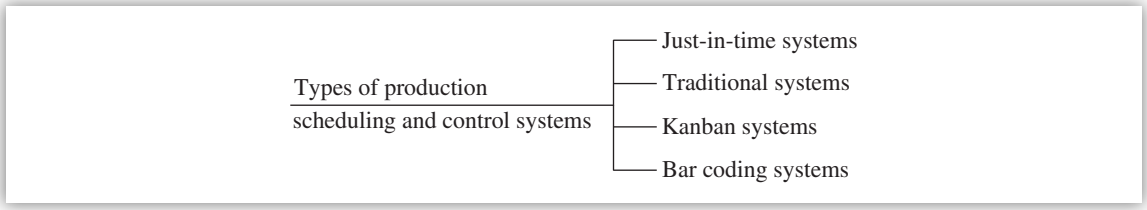


EXHIBIT 3.35 Types of Production Scheduling and Control Systems

(i) Just-in-Time Production Systems

JIT represents a management philosophy whose objective is to eliminate all sources of waste including unnecessary inventory. The basic principle of JIT is to produce the right products in the right quantity at the right time in the right place. JIT's primary goal is to minimize production inventory levels while providing needed raw materials, parts, and components just before they are used. To facilitate this goal, JIT purchasing places the orders such that delivery immediately precedes usage.

With JIT, products are manufactured or assembled only when they are needed. This means that the number of parts produced or purchased at any one time should be just enough to produce one unit of the finished product. Therefore, inventories are better managed to the extent that they are not needed or at least are minimized.

JIT AND RISK

JIT requires fundamental changes in traditional production systems. These changes encompass production layout, material flows, setup times, employee attitudes, and work culture. A risk of JIT is the critical dependency on a few vendors.

JIT requires a commitment to continuously improve activities and the quality of products while eliminating all non-value-added activities and work-in-process inventory. Lead times, waiting time for materials or other, and inspection are grouped as non-value-added activities.

Production flow in a JIT system is demand-pulled through the plant by the downstream workstations ordering subassemblies and parts from upstream workstations. These pull orders are controlled by a kanban system, which is a system of cards and empty bins. Kanban is explained later in the section.

JIT can be viewed as an intermediate step toward more advanced manufacturing technologies such as computer-integrated manufacturing. Producing one unit of a finished product at a time allows the implementation of strict quality control standards. The worker under JIT is fully responsible for ensuring that the subassemblies that are received or produced are error free. If errors are detected, production stops and errors are immediately corrected. *Therefore, the JIT system relies on employee involvement in production operations, quality control, and productivity improvements.*

KEY CONCEPTS TO REMEMBER: Benefits of JIT

- Increased inventory turnover measured as sales divided by inventory Increased inventory turnover is an indication of increased productivity
- Increased production rates due to little or no waiting time and increased productivity
- Lower storage space due to lower inventory levels required
- Lower spoilage costs due to high-quality products
- Lower material handling costs since the materials are delivered directly to the assembly floor

- Reduced production lead times due to shorter setup times and better coordination with suppliers
- Reduced indirect labor since most or all non-value-added activities are removed
- Reduced warranty claim costs due to better quality products

The total quality control system developed by D. Deming is an integral part of the JIT philosophy. Frederick Taylor's principles of scientific management influenced the development of the JIT system. Reduction of waste, zero inventories, quality circles, and the use of computer robotics are seen as management tools to increase efficiency and output—a theme familiar to scientific management and JIT production systems.

Raw material and WIP inventories are reduced significantly, thereby decreasing carrying costs and floor space requirements. JIT production systems are most appropriate in repetitive assembly type of manufacturing, such as automobiles or appliances.

The JIT system requires the setting of daily production targets, so that feedback on worker performance is timely. Workers are given more responsibility for building perfect quality into the product and producing the desired quantity. Detailed variance reports are no longer needed in JIT systems because defects become fewer and fewer.

JIT promotes work simplification procedures and relies on few suppliers to deliver raw materials and parts on time. Competitive bids are not common. Close ties tend to develop between two parties (customers and suppliers) as they work closely together to improve quality and to implement the JIT philosophy. JIT requires mutual trust between vendor and customer. The customer places greater reliance on the vendor to perform and deliver as expected.

(ii) Traditional Production Systems

Traditional production systems practice a "push" production system concept where each worker produces a subassembly at his or her own pace and passes the output to the next worker until the final product is completed. A WIP inventory is commonly maintained at each workstation. Plant workers are controlled by work standards and motivated by a piece-rate incentive system. This approach leads to producing quantity rather than quality products. Workers have little or no incentive to correct errors or problems.

Workers are encouraged to make good-quality products, not punished for the production of poor-quality work. Under a traditional production system, quality control is the responsibility of a quality control inspector, not the production worker. This quality control inspection is not done quickly enough to trace production problems. Inspection is not done continuously; it is often done for the finished goods only.

Work standards or standards of performance are established by using either imposition or via participation techniques, where the latter approach is more motivating for the worker than is the former. A performance report is issued periodically. A variance investigation occurs when significant discrepancies exist between the standard and the actual output. Investigation could reveal that either the worker is inefficient or the standard is not set properly. Exhibit 3.36 shows a comparison between traditional production systems and JIT production systems.

Characteristics of traditional production systems	Characteristics of JIT production systems
Quality is seen as a hit-or-miss event, and there is no explicit commitment to continuous improvement and production of quality products.	Quality is a planned event, and there is an explicit commitment to continuous improvement and production of quality products.
The system is evolutionary.	The system is revolutionary since long-held beliefs are discarded.
More WIP is maintained.	Little or no WIP is maintained.
There is no reliance on employee involvement and participation in decision making.	Systems rely on high employee involvement and participation in decision making.
Quality control inspector is responsible for the quality of the product.	Production worker is responsible for ensuring the quality of the product.
The push system begins with the first worker on the assembly line dictating the flow of work.	The pull system begins with the last worker on the assembly line dictating the flow of work.
Workers are compensated based on a piece-rate incentive system.	Workers are compensated based on a group incentive system.
Inventory investment is increased.	Inventory investment is decreased.
Need for detailed variance reports is great due to many defects. Reports are more useful as problem detectors.	There is little or no need for detailed variance reports due to fewer defects. Reports are less useful as problem detectors.
Long production runs and long setup times are typical.	Short production runs and short setup times are common.

EXHIBIT 3.36 Characteristics of Traditional Production Systems and JIT Production Systems

(iii) Kanban Production and Inventory System

Working under a "pull" system, production procedures and work instructions are communicated by a system of signals sent among workers through the use of a series of cards called *kanbans*. The JIT production system and kanban inventory system work together. In kanban, the last workstation is informed of the day's production needs; all other workstations respond to the kanban cards and containers (i.e., all other workstations are pulled in).

KEY CONCEPTS TO REMEMBER: Benefits of Kanban Inventory System

- Paperwork-free system
- Product made to order
- Diminished need to take physical inventory for income determination purposes
- Lower finished goods inventory amounts
- Simple procedures for taking physical inventory, when needed
- Lower WIP inventory amounts
- Zero or fewer defective products

After the kanban system informs the final assembly production needs, each workstation then "orders" products or parts from the preceding workstation. This chain moves back to the point of purchasing raw materials. One condition is that a workstation cannot produce unless an order has been placed.

Two kinds of kanban cards are used for posting and tracking inventory activity and to communicate among workers at the workstation: move cards and production cards (see Exhibit 3.37).

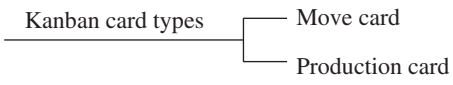


EXHIBIT 3.37 Kanban Card Types

The **move card** allows the worker to take one standard container of a specific part from one work center to another. The **production card** tells another production work center to produce the number of parts that will fit a standardized container. There is only one card with each container at any point in time.

MRP is a widely used computerized system that operates under the push principle, while kanban represents the pull system. The newer version of MRP is MRP II, which takes the BOM for the products to be produced and calculates all subassembly and raw materials needed by time and quantity. Then the workstations are informed as to the number of units to be produced. This method is equated to the push system where the work is pushed through the plant.

TRADITIONAL PRODUCTION SYSTEMS VERSUS MRP VERSUS JIT VERSUS KANBAN SYSTEMS

- A traditional manufacturing system practices a push production system.
- MRP systems operate under the push production system.
- A JIT manufacturing system practices a pull production system.
- A kanban manufacturing system practices a pull production system since it responds to the JIT production plan.

(iv) Bar Coding Systems

Sadhwani and Tyson[8] found that more and more managers are focusing on solutions that collect data in real time, at the point of origin, in a way that ensures the captured data are right the first time. One such solution is the use of automatic identification technologies, such as bar coding, optical character recognition (OCR), voice recognition (VR), and radio frequency (RF) identification. Of these methods, bar coding is the most popular and cost effective. Bar codes can be used in manufacturing environments, such as shop floor and receiving, as well as in office environments, such as purchasing, inventory, billing, accounts payable, and payroll time-clocking.

Bar codes are symbols that can be processed electronically to identify numbers, letters, or special characters on a receiving report, invoice, time card, or part. They are used to improve data

[8] Arjan T. Sadhwani and Thomas Tyson, "Bar Coding Technology: A Research Report," (Montvale, NJ: Institute of Management Accountants, 1990).

accuracy and increase speed of updating the supporting data in all interfacing systems. *Removing the human element from the data collection process greatly improves data accuracy and updating speed.*

Bar code technology supports the JIT production philosophy and continuous improvement program. This is because bar code technology is paperless, which is one of the goals of JIT. Bar codes support continuous improvement due to increased accuracy of data available in the system and establishment of production standards based on such data. This also improves quality of decision making. Exhibit 3.38 presents the advantages and disadvantages of bar code technology.

Advantages of bar coding technology	Disadvantages of bar coding technology
Improved employee productivity	High cost of equipment
Timeliness of data collection	Long implementation times
Accuracy of data collection	Continual support in education and training
Ability to trace labor and material costs directly to specific departments and jobs	Resistance to change by current employees

EXHIBIT 3.38 Advantages and Disadvantages of Bar Coding Technology

For example, the use of bar codes on raw materials reduces the amount of paperwork that is required to track inventories. Movement of raw materials, subassemblies, and finished products are monitored electronically using bar codes. In addition to speed, accuracy is increased since there is little or no human involvement in reading and interpreting the bar code data. Use of bar codes eliminates key entry of data.

3.6 Electronic Data Systems

The scope of electronic data systems includes a discussion of electronic funds transfer, electronic commerce, mobile commerce, electronic auctions, and electronic data interchange (EDI).

(a) Electronic Funds Transfer

Basically, an electronic funds transfer (EFT) system transfers money and other information electronically from one institution to another. A by-product of this service is the reduction of mountains of paper and time delays, thereby gaining cost efficiencies. For example, banks can transfer money from an account in one bank to another account in another bank, and the federal government can deposit benefits directly into recipients' bank accounts.

A trend in EFT systems is the transmittal of tax information electronically to tax authorities at a central processor. Information such as the amount, tax due, and employer identification number are provided to the central processor. Some advantages of this approach include fewer errors, lower costs, more timely deposits, and increased elimination of float associated with delays in moving funds.

Some state governments distribute public aid benefits electronically. Benefit recipients who use this system are given magnetic cards with their photographs, which they insert into special

electronic devices at the participating check-cashing centers or banks. The cards access computer records to tell the agents the amounts of benefits due.

Other applications include payment of unemployment insurance benefits. Claimants can call the government agency and enter their Social Security Number and personal identification number (PIN). After successfully answering certification questions, claimants are informed that they are to receive their benefits. Participants then gain access to their weekly payments with a plastic card and a PIN through automated teller machines (ATMs) or point-of-sale (POS) terminals. Those who already have a bank account are given the option to directly deposit their benefits, and those who prefer to receive state-issued checks may continue to do so. This is a clear example of integration of such diverse technologies such as POS, EFT, and ATMs.

(b) Electronic Commerce

(i) Overview

Electronic commerce (e-commerce) is defined as a place where buyers and sellers are connected using computers and networks (the Internet) to buy and sell goods and services. The term "electronic business" (e-business) is much broader than e-commerce because the former includes distribution of information and customer support, which are lacking in the latter. In other words, e-commerce is a subset of e-business.

E-COMMERCE AND VALUE CHAIN

E-commerce is a Web-enabled value chain since the Internet is the enabling technology. Business applications are located on Web servers for wide access to employees and selective access to customers and suppliers.

A **value chain** is created in e-commerce among demand planning, supply planning, and demand fulfillment. Demand planning consists of analyzing buying patterns and developing customer demand forecasts. Supply planning consists of supply allocation, inventory planning, distribution planning, procurement planning, and transportation planning. Demand fulfillment consists of order capturing, customer verification, order promising, backlog management, and order fulfillment.

(ii) Electronic Commerce Models

Several e-commerce models exist, including business-to-consumer (B2C), business-to-business (B2B), consumer-to-consumer (C2C), government-to-citizen (G2C), government-to-business (G2B), consumer-to-business (C2B), and exchange-to-exchange (E2E) models.

- In the B2C model, online retail stores sell goods directly to consumers. EDI is a critical component of the sales process for many online retailers.
- In the B2B model, the Internet enables existing relationships between two companies in exchanging goods and services. EDI is the underlying technology in both B2C and B2B, enabling online catalogs and continuous stock replenishment programs.
- In the C2C model, consumers buy and sell goods with other consumers through auction sites (e.g., eBay).

- In the G2C model, the federal government uses the Internet to reach citizens for a variety of information-dissemination purposes and transactions (e.g., Internal Revenue Service, U.S. Postal Service, Medicare and Medicaid, and Social Security Administration).
- In the G2B model, all levels of government deals with business entities to procure goods and services (e-procurement).
- In the C2B model, mostly individual consumers and some businesses request lower prices for airline tickets, hotels, car rentals, vacations, and resorts from selling companies, and these companies come back with the lowest price.
- In the E2E model, the electronic exchanges formally connect to one another for the purpose of exchanging information (e.g., stock brokers/dealers with stock markets and vice versa).

(iii) E-Commerce Security Risks and Controls

E-commerce security risks arising from technical threats include denials of service, zombies, phishing, Web server and Web page hijacking, botnets, and malicious code (e.g., viruses, worms, and Trojan horses). Risks arising from nontechnical threats include pretexting (impersonating) and social engineering.

E-commerce requires robust authentication due to potential risks such as cyberattacks and intrusions. The next security controls help to prevent and detect such attacks and intrusions:

- Multifactor authentication methods
- One-time passwords
- Continuous authentication with digital signatures and digital certificates
- Defense-in-depth strategies
- Need-to-know and least-privilege access privileges
- Role-based access controls
- Logging and monitoring practices
- Software patch management program
- Security incident response handling capabilities

(iv) E-Commerce Security Classes

For the purposes of exploring the relevant security issues, e-commerce can be divided into four basic classes: (1) electronic mail (e-mail), (2) EDI, (3) information transactions, and (4) financial transactions.

$$\begin{aligned}\text{E-commerce security issues} = {} & \text{E-mail security issues} + \text{EDI security issues} \\ & + \text{Information transaction security issues} \\ & + \text{Financial transaction security issues}\end{aligned}$$

(A) E-mail Security Issues The use of Internet e-mail to carry business-critical communications is growing exponentially. While e-mail provides a low-cost means of communication with customers, suppliers, and partners, a number of security issues are related to the use of e-mail. The security issues include:

- Internet e-mail addresses are easily spoofed. It is nearly impossible to be certain who created and sent an e-mail message based on the address alone.

- Internet e-mail messages can be easily modified.
- Standard Simple Mail Transfer Protocol (SMTP) mail provides no integrity checking.
- There are a number of points where the contents of an e-mail message can be read by unintended recipients.
- There is usually no guarantee of delivery with Internet e-mail. While some mail systems support return receipts, when such receipts work at all they often signify only that the user's server (not necessarily the user) has received the message.

These weaknesses make it important for organizations to issue policies defining acceptable use of e-mail for business purposes.

(B) Electronic Data Interchange Security Issues Traditional EDI systems allow preestablished trading partners to electronically exchange business data through value-added networks (VANs). The Internet can provide the connectivity needed to support EDI at a substantial cost savings over VANs. However, the Internet does not provide the security services (integrity, confidentiality, and nonrepudiation) required for business EDI. Similar to e-mail over the Internet, EDI transactions are vulnerable to modification, disclosure, or interruption when sent over the Internet. The use of cryptography to provide the required security services has changed this; consequently, many companies and government agencies are moving to Internet-based EDI.

SCOPE OF E-COMMERCE

E-commerce encompasses a broader commerce environment than EDI. Because of this, EDI is a subset of e-commerce. Similarly, e-commerce is a subset of e-business.

(C) Information Transactions Security Issues Providing information (e.g., stock quotes, news) is a major and costly element of commerce. Using the Internet to provide these services is substantially less expensive than fax, telephone, or postal mail services. Integrity and availability of the information provided are key security concerns that require security controls and policy.

(D) Financial Transactions Security Issues Computer networks are used to process financial transactions, such as checks, debit cards, credit cards, and EFT. Similar to EDI over VANs, the connectivity options have been limited, and leased lines are expensive. The Internet provides an opportunity for cost savings in electronic financial transactions. The use of the Internet to carry these types of transactions replaces the physical presentation or exchange of cash, checks, or debit/credit cards with the electronic equivalent. Each of these forms of transactions involves the use of cryptography to provide for integrity, confidentiality, authentication, and nonrepudiation. For example, a standard known as secure electronic transactions (SET) is used for processing credit card transactions over public networks. Use of SET involves three-way transactions among buyer, seller, and a financial institution (a bank).

(v) E-Commerce Software

E-commerce software should support these tasks:

- **Catalog management.** Catalog management software combines different product data formats into a standard format for uniform viewing, aggregating, and integrating catalog

data into a central repository for easy access, retrieval, and updating of pricing and availability changes.

- **Product configuration.** Customers need help when an item they are purchasing has many components and options. Buyers use the new Web-based product configuration software to build the product they need online with little or no help from salespeople.
- **Shopping cart facilities.** Today many e-commerce sites use an electronic shopping cart to track the items selected for purchase, allowing shoppers to view what is in their cart and add new items or remove items from it.
- **E-commerce transaction processing.** E-commerce transaction processing software takes data from the shopping cart and calculates volume discounts, sales tax, and shipping costs to arrive at the total cost.
- **Web site traffic data analysis.** Web site traffic data analysis software captures visitor information, including who is visiting the Web site, what search engine and key words they used to find the site, how long their Web browser viewed the site, the date and time of each visit, and which pages were displayed. These data are placed into a Web log file for future analysis to improve the Web site's performance.

(vi) E-Commerce Infrastructure

Key technology infrastructure for e-commerce applications include Web server hardware, server operating system, server software, e-commerce software, virtual private network (VPN), value-added network (VAN), and the Internet, intranet, or extranet. Strategies for successful e-commerce include: (1) developing an effective Web site that creates an attractive presence and that meets the needs of its visitors (customers); (2) contracting out with Web site hosting service providers or storefront brokers; (3) building traffic into the Web site through a metatag, which is a special hypertext markup language (HTML) tag that contains keywords about the Web site; and (4) analyzing Web site traffic to identify which search engines are effective for your business.

Examples of Best Practices in Electronic Commerce

- There should be a set of security mechanisms and procedures that, taken together, constitute a security architecture for e-commerce (deals with architecture).
- There should be measures in place to ensure the choice of the correct protocols for the application and the environment as well as the proper use and exploitation of their features and compensation for their limitations (deals with infrastructure/protocol).
- There should be a mechanism in place to mediate between the public network (the Internet) and an organization's private network (deals with infrastructure or firewall).
- There should be a means to communicate across the Internet in a secure manner (deals with infrastructure/virtual private network).
- There should be a process whereby participants in an e-commerce transaction can be uniquely and positively identified (deals with authentication/digital certificates).
- There should be a mechanism by which the initiator of an e-commerce transaction can be uniquely associated with it (deals with authentication/digital signatures).
- There should be an infrastructure to manage and control public key pairs and their corresponding certificates (deals with authentication/public key infrastructure [PKI]).
- There should be procedures in place to control changes to an e-commerce presence (deals with applications/change control).

- E-commerce applications should maintain logs of their use, which should be monitored by responsible personnel (deals with applications/logs and monitoring).
- There should be methods and procedures to recognize security breaches when they occur (deals with applications/intrusion detection).
- There should be features in e-commerce applications to reconstruct the activity performed by the applications (deals with applications/auditability).
- There should be a means to maintain a provable association between an e-commerce transaction and the person who entered it (deals with applications or nonrepudiation).
- There should be protections in place to ensure that data collected about individuals are not disclosed without their consent or used for purposes other than that for which they were collected (deals with applications/privacy).
- There should be a means to ensure the confidentiality of data communicated between customers and vendors (deals with data protection/encryption).
- There should be mechanisms to protect e-commerce presences and their supporting private networks from computer viruses and to prevent them from propagating viruses to customers and vendors (deals with data protection/virus scanning).
- There should be protection over the devices used to access the Internet (deals with availability/protecting the user environment).
- There should be features within e-commerce architecture to keep all components from failing and for components to repair themselves if they should fail (deals with availability/fault tolerance).
- There should be a plan and procedures to continue e-commerce activities in the event of an extended outage of required resources for normal processing (deals with availability/business continuity planning).
- There should be a commonly understood set of practices and procedures to define management's intentions for the security of e-commerce (deals with policy and governance/policy).
- There should be measures in place to prevent information about customers from being disclosed and not used for purposes other than that for which it was obtained, without the customer's permission (deals with policy and governance or privacy).
- There should be shared responsibility within an organization for e-commerce security (deals with policy and governance/oversight).
- There should be communication from vendors to customers about the level of security in an e-commerce presence (deals with policy and governance or notification).
- There should be a regular program of audit and assessment of the security of e-commerce environments and applications to provide assurance that controls are present and effective (deals with policy and governance/auditing and assurance).

Source: E-Commerce Security, Enterprise Best Practices, Information Systems Audit and Control Research Foundation (ISACRF), now known as the IT Governance Institute, Rolling Meadows, IL, 2000.

(c) Mobile Commerce

Mobile commerce (m-commerce), which is an extension of e-commerce, is conducted using mobile devices such as cell phones and tablets for wireless banking and shopping purposes. M-commerce uses wireless application protocol (WAP). M-commerce is any business activity conducted over a wireless telecommunications network. Both B2B and B2C e-commerce

transactions can use m-commerce technology. Security risks and controls for m-commerce are similar to those of e-commerce.

(d) Electronic Auctions

Another extension of e-commerce is electronic auctions (e-auctions), which are conducted online through the Internet. Near-perfect market information is available about prices, products, current supply, and current demand, which benefits all parties. Several variations of e-auctions exist:

- A seller invites consecutive bids from multiple buyers, and the bidding price either increases or decreases sequentially (forward auction). This is a model of one seller and many buyers. The forward auction is practiced mostly with the C2C e-commerce model.
- A buyer invites bids, and multiple sellers respond with the price reduced sequentially, and the lowest bid wins (backward or reverse auction). This is a model of one buyer and multiple sellers. The reverse auction is practiced with B2B, G2B, and C2B e-commerce models.
- Multiple buyers propose bidding prices, and multiple sellers respond with asking prices simultaneously. Both prices are matched based on the quantities of items available on both sides (double auction). This is a model of many buyers and many sellers.
- Negotiations and bargaining power can take place between one buyer and one seller due to supply and demand. This is a model of one buyer and one seller.
- Sellers and buyers interact in one industry or for one commodity (vertical auction). Prices are determined dynamically through the bidding process.

Limitations of e-auctions include minimal security for C2C auctions (i.e., no encryption), possibility of fraud (i.e., shipping defective products), and limited buyer participation because the e-auctions may be invitation only or open to dealers only. B2B, G2B, and C2B auctions are secure due to use of private, leased lines.

(e) Electronic Data Interchange

EDI systems provide computer-to-computer communication. EDI systems are becoming a normal way of exchanging or transmitting documents, transactions, records, quantitative and financial information, and computer-related messages from one computer to another. Some examples of transactions and documents involved include purchase orders, invoices, shipping notices, receiving advice, acknowledgments, and payments. When payment is involved, the EDI system can be referred to as an EFT system.

EDI is replacing manual data entry with electronic data entry. The objective of EDI is to eliminate manual data entry work and to eliminate or reduce paper mailing and processing delays between two trading parties (e.g., buyer and seller, manufacturer and supplier).

Traditional paper-driven systems, such as order entry, purchase order, billing, and accounts payable systems, are changing significantly with the introduction of EDI-based systems. Some problems with traditional paper-driven application systems are low accuracy, increased mailing and processing times, and high labor and processing costs.

Basically, the transmission of information between two parties can take place in three ways: (1) direct, (2) via a third-party service provider, and (3) in the form of computer tapes, disks, and diskettes.

(i) EDI System

Essentially, the EDI system works in this way:

- The buyer identifies the item to be purchased. Data are entered into the purchasing application system. Translation software creates an EDI purchase order, which is sent electronically to the supplier. The same order is sent to the buyer's accounts payable and goods receiving system.
- A functional acknowledgment, indicating receipt of the order, is automatically generated and electronically transmitted to the buyer.
- The supplier's computer sends the order information to the supplier's shipping and invoicing systems.
- When the buyer receives the ship notice, the data are electronically entered into the receiving system file.
- The receipt notice is electronically transmitted to the accounts payable application system.
- The ship notice is electronically transmitted to the invoicing application system.
- An invoice is electronically generated by the supplier and transmitted to the buyer. The same information is sent to the supplier's accounts receivable system.
- The invoice is received by the buyer's computer and is translated into the buyer's format. The invoice, receiving notice, and purchase order are electronically matched and reconciled.
- The buyer electronically transmits payment to the supplier's bank through their bank. An electronic remittance advice is transmitted to the supplier.
- Upon receipt of the remittance and notice of payment, the data are transmitted into the accounts receivable system, and the buyer account is updated. The buyer is given credit for payment.

(ii) Components of an EDI System

The components of an EDI system are standards, software, and networks. The EDI **standards** consist of formatting standards and communication standards. Formatting standards deal with the type, sequence, and content of an electronic document. Communication standards cover baud rate, protocols, electronic envelopes, and message transmission times. Standards provide a set of common rules, in terms of syntax and formatting, for the development of electronic communications.

In terms of **software**, a translation program is needed to translate company-specific data to EDI standard format for transmission. A reverse translation is performed when data arrive at the organization from external sources.

In terms of **networks**, there are two approaches in common use. In a direct network, the computers of the trading partners are linked directly, usually through dial-up modems. A direct network is effective for a limited number of trading partners. As the number of trading partners increases, it is difficult to maintain open lines for all trading partners. The second choice is to use a third-party network (VAN) that acts as an intermediary between trading partners. A VAN maintains a mailbox for both the sender and the receiver.

The VAN receives purchase orders from the sender (buyer), sorts them by seller, and places each seller's purchase orders in his mailbox. At a later time, the seller can dial in to the VAN and

retrieve its mail in the form of electronic purchase orders. This approach allows each trading partner to create only one electronic transmission to the VAN rather than each trading partner having to create a separate electronic transmission.

(iii) Benefits of EDI

A major benefit of EDI is being able to load data, without rekeying, from various formats and place it where it is needed in a different format for further processing. Besides savings due to reductions in document mailing and processing costs, decreases in data entry personnel costs, and reductions in inventory stock levels, organizations are realizing other significant benefits.

These added benefits include:

- Improved operational efficiency in warehousing, shipping, purchasing, and receiving areas.
- Increased sales.
- Increased customer responsiveness.
- Increased ability to compete.
- Quick access to better information in a timely manner.

The users of EDI include organizations in the trucking, retail, shipping, grocery, health care, pharmaceutical, and automotive industries, government, and others.

3.7 Business Development Life Cycles

Topics such as phases of business development life cycles and causes and activities behind those cycles are discussed. In addition, how consumer durable and nondurable goods are affected in business cycles is explained. Growth concepts between a company and the nation are compared.

(a) Overview

Any nation seeks economic growth, full employment, and price level stability. However, achieving full employment and price level stability is not steady or certain. In the United States, both unemployment and inflation have threatened or interrupted the long-term trend of economic growth.

The **business cycle** refers to the recurrent ups and downs in the level of economic activity that extends over time. Economists suggest four phases of the business cycle: peak, recession, trough, and recovery (see Exhibit 3.39). The duration and strength of each phase is variable. Some economists prefer to talk about business fluctuations rather than cycles because cycles imply regularity while fluctuations do not.

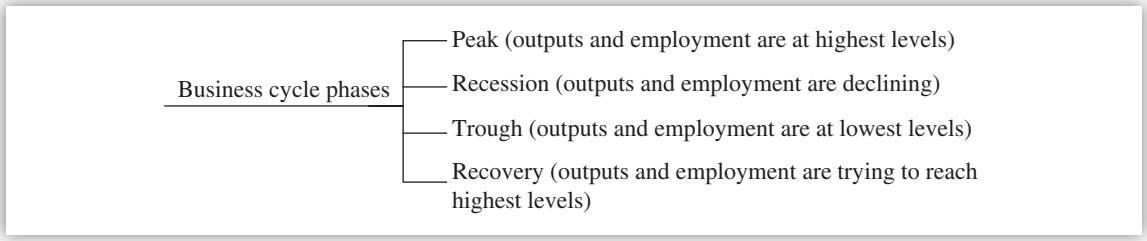


EXHIBIT 3.39 Business Cycle Phases

- **Peak.** The economy is at full employment, and the national output is close to capacity. Price levels are likely to rise.
- **Recession.** Both output and employment decline, but prices tend to be relatively inflexible in a downward direction. Depression sets in when the recession is severe and prolonged, and prices fall. In an economy experiencing a recession with low inflation, the central bank could stimulate the economy by purchasing securities in the secondary market, which will increase money supply.
- **Trough.** Both output and employment bottom out at their lowest levels.
- **Recovery.** Both output and employment expand toward full employment. As recovery intensifies, price levels may begin to rise prior to the realization of full employment and capacity production.

(b) Causes behind the Business Cycles and Business Activity

Economists offer many theories supporting the reasons behind the nature of the four phases of the business cycle and its impact on business activity. Examples are listed next.

- Innovations (e.g., computers, drugs, synthetic fibers, automobiles) have greater impact on investment and consumer spending, and therefore on output, employment, and the price level. This innovation is not regular and continued.
- Political and random events, such as wars, have a major impact on increasing employment and inflation followed by slump when peace returns.
- The government's monetary policy has a major impact on business activity. When a government creates too much money, inflation results. When a government restricts money supply, lower output and unemployment result.
- The level of total expenditures has a major impact on the levels of output and employment.

KEY CONCEPTS TO REMEMBER: Total Expenditures

- When total expenditure is low, output, employment, and incomes will be low. Less production will be profitable to the business.
- When total expenditure is high, output, employment, and incomes will be high. More production will be profitable to the business.

- Many businesses, such as retail, automobile, construction, and agriculture, are subject to seasonal variations (e.g., pre-Christmas, pre-Easter).
- Business activity is also subject to a secular trend. The secular trend of an economy is its expansion or contraction over a long period of time (i.e., 25 or more years). Both seasonal variations and secular trends are due to noncyclical fluctuations.

It is important to note that various individuals and various segments of the economy are affected in different ways and in different degrees by the business cycle. For example, consumer durable and consumer nondurable goods industries are affected in different ways, as explained next.

- **Consumer durable.** Those industries producing heavy capital goods and consumer durables (e.g., household appliances, automobiles), called hard goods industries, are highly sensitive to the business cycle. Both production and employment will decline during recession and increase during recovery.

  The reason for sensitivity of the consumer durable industry is that consumers and producers alike can postpone the purchase of hard goods. Producers do not invest in capital goods during recession and postpone investment until the economy gets better. Consumers also postpone the purchase of hard goods during recession and prolong the life of hard goods by repairing old appliances and automobiles rather than buying new models. Producers cut the output and employment instead of lowering prices due to their concentration in the industry. Price cuts could be modest, even if they occur.

- **Consumer nondurables.** Output and employment in nondurable consumer goods industries are less sensitive to the business cycle. This is because food and clothes, which are examples of the consumer nondurable industry, are simply necessities of life. These are called soft good industries. Because it is a highly competitive and low-concentration industry, prices will be cut instead of production and employment. Production decline would be modest, even if it occurs.

Financial managers need to develop financial forecasts and capital investment plans according to the phase of the business cycle the firm is going through and the type of industry the firm belongs to (i.e., whether consumer durables or consumer nondurables).

(c) Growth Concepts

Another interesting concept is to compare the growth of a firm with that of the economy. Four growth concepts emerge: supernormal growth, normal growth, zero growth, and negative growth (see Exhibit 3.40). Each growth concept is briefly explained next.

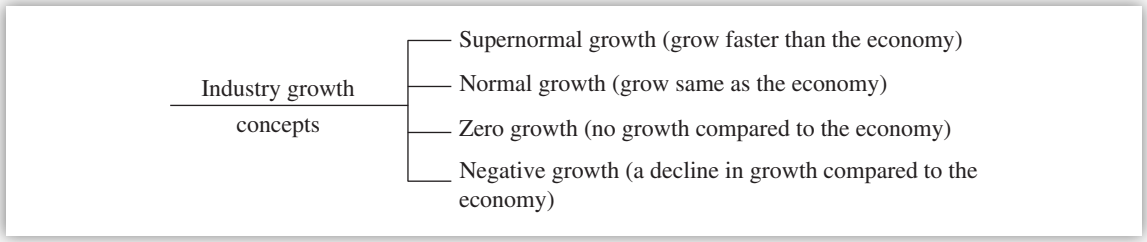


EXHIBIT 3.40 Industry Growth Concepts

- **Supernormal growth** is the part of the life cycle of a firm in which its growth is much faster than that of the economy as a whole.
- **Normal growth** is growth that is expected to continue into the foreseeable future at about the same rate as that of the economy as a whole. The growth rate of a firm is equal to the nominal gross national product (GNP), which is real GNP plus inflation.
- **Zero growth** indicates that a firm experiences a 0% growth compared to the economy as a whole.
- **Negative growth** indicates that a firm experiencing a decline in growth compared to the economy as a whole.

3.8 International Organization for Standardization Framework

The International Organization for Standardization (known as ISO) framework consists of a series of global standards with appropriate guidelines published by the ISO in Switzerland. The ISO only develops and publishes standards for which there is a clear market requirement (www.iso.org).

ISO standards provide solutions and achieve benefits for almost all sectors of activity in a nation, including agriculture, construction, mechanical engineering, manufacturing, distribution, transport, health care, information and communication technologies, the environment, energy, safety and security, quality management, and services.

ISO 9000 is the major standard in quality management. It addresses quality system processes, not product performance specifications. In other words, ISO 9000 covers how products are made and services are rendered but not necessarily how they work. ISO 9000 focuses on processes, not on products, services, or people. It is based on the concept that fixing the process will fix the product or service. ISO 9000 is a standard to judge the quality of suppliers. It assumes that suppliers have a sound quality system in place and it is being followed. ISO 9000 can be used as a baseline quality system to achieve total quality management (TQM) objectives and Six Sigma goals.

ISO standards are becoming an acceptable worldwide approach to vendor certification and international trade. The real push is from companies throughout the world that are requesting that their suppliers become certified. ISO 9000 standards are equally applicable to manufacturing and service industries and remove the nontariff barriers that arise from differences and inadequacies among national, local, or company standards. Major categories of nontariff barriers include quantitative import restrictions, such as quotas, voluntary export restraints, and price controls. However, the ISO 9000 standards cannot remove each government's tariffs (taxes placed on imported goods to raise revenues and protect domestic industries from foreign competition).

(a) ISO Certification Process

To earn ISO 9000 certification, a company must set up and document all procedures that relate to the process to be certified. These procedures can include everything from procuring and storing raw materials, to designing products, to issuing change orders on designs, to controlling inventory, to answering customer phone calls. Flowcharts can be used to document the procedures in place.

Documentation of these procedures ensures that they are followed throughout the organization. The idea is that by rethinking and documenting every step of the corporate process, companies can identify and eliminate trouble spots, such as non-value-added activities and waste, and thus improve overall quality. *The probability of producing a high-quality product increases because the risk that leads to poor quality declines as the processes are documented and followed. ISO 9000 forces discipline into the system.*

After an application for certification is filed, registrars or auditors accredited by a national quality board will conduct on-site audits. During the audit, registrars ask questions about company procedures and policies.

(b) Overall Benefits of ISO Standards

International standards bring technological, economic, and societal benefits. They help to harmonize technical specifications of products and services, making industry more efficient and breaking down barriers to international trade. Conformity to international standards helps reassure consumers that products are safe, efficient, and good for the environment. However, ISO does not provide certification or conformity assessment. Companies need to contact an external certification body for that.

(i) For Businesses

International standards are strategic tools and guidelines to help companies tackle some of the most demanding challenges of modern business. They ensure that business operations are as efficient as possible, increase productivity and help organizations access new markets. Businesses also benefit from taking part in the standard development process. Standards share best practices so that organizations do not reinvent the wheel. They help reduce waste, provide better results, and increase interoperability, efficiency, and compatibility. They facilitate market access for innovations and empower companies to compete globally. Examples of benefits for businesses include:

- **Cost savings.** International standards help optimize operations and therefore improve the bottom line.
- **Enhanced customer satisfaction.** International standards help improve quality, enhance customer satisfaction, and increase sales.
- **Access to new markets.** International standards help prevent trade barriers and open up global markets.
- **Increased market share.** International standards help increase productivity and competitive advantage.
- **Environmental benefits**. International standards help reduce negative impacts on the environment.

(ii) For Consumers

When products and services conform to international standards, consumers can have confidence that they are safe, reliable and of good quality. For example, ISO standards on road safety, toy safety, and secure medical packaging are just a selection of those that help make the world a safer place. International standards on air, water and soil quality, on emissions of gases and radiation, and environmental aspects of products contribute to efforts to preserve the environment and the health of citizens.

(iii) For Government

ISO standards draw on international expertise and experience and are therefore a vital resource for governments when developing regulations. National governments can make ISO standards a regulatory requirement (remember, ISO standards themselves are voluntary). This has a number of benefits:

- **Expert opinion.** ISO standards are developed by experts. By integrating an ISO standard into national regulations, governments can benefit from the opinion of experts without having to call on their services directly.

- **Opening up world trade.** ISO standards are international and adopted by many governments. By integrating ISO standards into national regulation, governments help to ensure that requirements for imports and exports are the same the world over, thereby facilitating the movement of goods, services, and technologies from country to country.

(iv) Reducing Technical Barriers to Trade

The existence of different national or regional standards can create technical barriers to trade and increase the cost of doing business. International standards provide the technical basis on which political trade agreements can be put into practice, whether they are at the regional or international level. The ISO/IEC (International Electrotechnical Commission) 17021:20011 Conformity Assessment standard can serve as a foundation to facilitating international trade.

(c) Specific Benefits of ISO 9000 Standards

The painstaking certification process yields several benefits for customers of certified manufacturers and service providers. These benefits include:

- Products from ISO 9000-certified suppliers are likely to be more reliable.
- When every step of a manufacturing process is documented, it is easier to spot problems and trace them back to an exact point in the manufacturing line. Problem tracking is facilitated.
- Its document-it-all approach makes it easier for users to evaluate products and services and to anticipate potential problems.
- Costs will be lower for both the manufacturer and the customer due to efficient operations. Lower design costs translate to lower product costs, which should mean lower prices for users.
- Buying products from ISO-certified suppliers can save customers the time and expense of conducting on-site visits of manufacturing facilities.
- Not having to test incoming parts from ISO-certified suppliers because suppliers' procedures include testing saves time and money.

(d) Specific ISO Standards

Specific ISO standards discussed in this section include the following:

- ISO 9000 — Quality Management
- ISO 14000 — Environmental Management
- ISO 17021 — Conformity Assessment
- ISO 21500 — Project Management
- ISO 22000 — Food Safety Management
- ISO 22301 — Business Continuity Management
- ISO 26000 — Social Responsibility
- ISO 27001 — Information Technology Security Techniques—Requirements of Information Security Management Systems

- ISO 27002 — Information Technology Security Techniques—Code of Practice for Information Security Management
- ISO 28000 — Security Management Systems for the Supply Chain
- ISO 31000 — Risk Management
- ISO 50001 — Energy Management
- Other ISO standards related to IT

(i) ISO 9000 – Quality Management

The ISO 9000 family of standards addresses various aspects of quality management and contains some of ISO's best-known standards. The standards provide guidance and tools for all organizations that want to ensure that their products and services consistently meet customers' requirements and that quality is consistently improved. The ISO 9000 family addresses quality management. This means what the organization does to fulfill customers' quality requirements and applicable regulatory requirements, while aiming to enhance customer satisfaction and achieve continual improvement of its performance in pursuit of these objectives. Note that the ISO is an independent organizational body that develops and publishes the standard; it does not "certify" individual user organizations.

There are many standards in the ISO 9000 family:

- ISO 9000:2005 covers the basic concepts and language.
- ISO 9001:2008 sets out the requirements of a quality management system (QMS), which is also used in the supply chain to select suppliers.
- ISO 9004:2009 focuses on how to make a QMS more efficient, effective, and sustainable.
- ISO 19011:2011 sets out guidance on internal and external audits of QMS and environmental management systems.

The correct sequence of flow of the ISO 9000 family of standards is shown next:

$$\text{ISO 9000} \rightarrow \text{ISO 9001} \rightarrow \text{ISO 9004} \rightarrow \text{ISO 19011}$$

The **ISO 9000 standard** provides the fundamentals and vocabulary used in the entire ISO 9000 family of standards. It sets the stage for understanding the basic elements of QMS. It starts with overall requirements as inputs; management responsibility, focus, policy, planning, and objectives; resource management and allocation; product realization and process management; measurement, monitoring, analysis, and improvement; products as outputs; and continual improvement.

The **ISO 9001 standard** is used when a company is seeking to establish a QMS that provides confidence in an organization's ability to provide products and services that fulfill customer needs and expectations (i.e., customer satisfaction). The term "product" applies to services, processed materials, hardware, and software intended for customers. ISO 9001 does not specify requirements for the goods or services that buyers seek to purchase. Instead, a buyer needs to refer to product specifications, drawings and blueprints, national or international product standards, supplier's catalogs, or other documents to specify requirements.

ISO 9001:2008 is the standard that provides a set of standardized requirements (criteria) for a QMS and supply chain, regardless of what the user organization does, its size, or whether

it is the private or public sector. It is the only standard in the 9000 family against which all organizations can be certified—although certification is not a compulsory requirement of the standard. It can be used by any organization large or small, regardless of its field of activity. The standard is based on a number of quality management principles, including a strong customer focus, the motivation and implication of top management, the process approach, and continual improvement. Using ISO 9001:2008 helps ensure that customers get consistent good-quality products and services, which in turn brings many business benefits. Checking that the system works is a vital part of ISO 9001:2008, and it can be certified by an external auditing body. ISO 9001 is the only standard in the ISO family that can be used for the purpose of conformity assessment.

WHAT ARE THE WAYS TO ESTABLISH A SUPPLIER'S CONFORMITY ASSESSMENT TO ISO 9001?

Buyers can ask suppliers whether the goods and services that they are trying to acquire from suppliers are covered by the supplier's QMS. Do not hesitate to ask for a copy of the supplier's actual certificate or declaration of conformity as proof of evidence. Note that a statement of conformity to ISO 9001 by a supplier should not, however, be considered a substitute for a declaration or statement of product conformity. Refer to ISO/IEC 17021:2011 standard "Conformity Assessment—Requirements for Bodies Providing Audit and Certification of Management Systems" for additional guidance.

Possible options exist to establish a supplier's conformity assessment. These include:

- A user organization by itself performing a self-assessment audit against 9001:2008 to verify that it is managing its processes effectively and controlling its activities efficiently. This is not an objective evaluation.
- A supplier's declaration or statement of product conformity by itself affirming that its QMS meets the ISO 9001:2008 requirements through the supplier's internal audit, a second-party audit, or a third-party audit.
- A second-party assessment conducted by a supplier's customers or clients stating that the work complies with QMS and meets the ISO 9001:2008 requirements that are used in their contractual B2B transactions.
- Third-party assessments where a supplier hires an impartial third party, such as a certification body or registrar, to issue a certificate of conformity that complies with the ISO 9001:2008 requirements. Additional confidence can be obtained by an accredited certification body or registrar who verifies that the certification body is independent and competent to carry out the certification process as per the ISO 9001:2008 requirements.

The last option has proved extremely popular in the marketplace because of the perceived credibility of an independent assessment. The user organization may thus avoid multiple audits by its clients or reduce the frequency or duration of client audits. The certificate of conformity can also serve as a business reference document between the user organization and potential clients, especially when suppliers and clients are new to each other or when they are local or global.

The **ISO 9004 standard** is used to extend the benefits obtained from ISO 9001 to all parties that are interested in or affected by an organization's operations. Interested parties include employees, owners, suppliers and vendors, business partners, and society in general. The ISO 9001 and the ISO 9004 standards are compatible and can be used separately or in combination to meet or exceed expectations of customers and interested parties. Both standards apply a process approach such as PDCA cycle framework.

Furthermore, the ISO 9004 standard gives guidance on a wider range of objectives of a QMS than does ISO 9001, particularly in managing for the long-term success of an organization. ISO 9004 is recommended as a guide for organizations whose top management wishes to extend the benefits of ISO 9001 in pursuit of systematic and continual improvement of the organization's overall performance. However, ISO 9004 is not intended for certification or contractual purposes.

The **ISO 10014 standard** provides guidelines for realizing financial and economic benefits from the application of the ISO 9000 quality management principles. It is directed to top management of the organization and complements the ISO 9004 for performance improvements.

The **ISO 19011 standard**, when combined with ISO/IEC 17021 standard, covers the area of auditing of QMS and environmental management system (EMS). It provides guidance on the audit programs, the conduct of internal or external audits, and information on auditor competence. ISO 19011 provides an overview of how an audit program should operate and how management system audits should take place. Effective audits ensure that an implemented QMS meets the requirements specified in ISO 9001. An organization must perform internal audits to check how its QMS is working. An organization may decide to invite an independent certification body to verify that it is in conformity to the standards, but there is no requirement for this. Alternatively, it might invite its clients to audit the quality system for themselves.

ISO/TS 16949:2002 deals with QMS regarding requirements for the application of ISO 9001:2000 for the automotive industry and relevant service part organizations.

(A) Implementing and Maintaining a QMS Implementing and maintaining a QMS based on the ISO 9001 standard requires seven steps:

1. Fully engage top management to define mission, vision, values, stakeholders, policies, and product or service quality objectives.
2. Identify key processes and the interactions needed to meet quality objectives.
3. Implement and manage the QMS and its processes, using process management techniques,
4. Build ISO-9001-based QMS using a fit-gap analysis to identify where existing system requirements are fulfilled and where they are not.
5. Implement the system, train company staff, and verify effective operations of the processes.
6. Manage the QMS with a focus on customer satisfaction, strive for continual improvement, and implement business excellence models.
7. If necessary, seek third-party certification/registration of the QMS or, alternatively, issue a self-declaration of conformity.

(ii) ISO 14000 – Environmental Management

The ISO 14000 family of standards addresses various aspects of EMS. This means what the organization does to minimize harmful effects on the environment caused by its activities and to achieve continual improvement of its environmental performance. These standards provide practical tools for organizations looking to identify and control their environmental impact and

constantly improve their environmental performance. Both ISO 14001 and ISO 14004 focus on environmental management systems and deal with the PDCA cycle framework.

Examples of ISO 14000 family of standards are described next.

(A) ISO 14000 Standard ISO 14000 is the international standard for EMS. The scope includes all the efforts to minimize waste and redesign manufacturing processes, products, and packaging to prevent pollution. More attention should be placed on pollution prevention rather than correction. To achieve these goals, environmental protection, like quality, safety, and security management, must be integrated into daily business operations.

(B) ISO 14001 Standard ISO 14001 is a national standard and is a management framework for planning, developing, and implementing environmental strategies in an organization. The framework includes a policy, a planning process, an organizational structure, specific objectives and targets, specific implementation programs, communications and training programs, and management review, monitoring, and corrective action, which includes environmental audit. The standard is applicable to any organization regardless of size or business type. Note that ISO 9001 and ISO 14001 are compatible in design and structure, and audits.

(C) ISO 14001:2004 ISO 14001:2004 identifies and controls the environmental impact of its activities, products, or services; improves its environmental performance continually; implements a systematic approach to setting environmental objectives and targets; and demonstrates that targets have been achieved. It is not the intention of this standard to specify levels of environmental performance because they are too specific and detailed for each business activity. This standard provides a generic framework of requirements for a holistic, strategic approach to an organization's environmental policies, plans, and actions.

The ISO14001:2004 standard has the effect of establishing a common reference for communicating about environmental management issues among organizations and their customers, regulators, the public, and other stakeholders. Because this standard does not lay down levels of environmental performance, it can be implemented by a wide variety of organizations, whatever their current level of environmental maturity. However, a commitment to compliance with applicable environmental legislation and regulation is required, along with a commitment to continual improvement—for which the environmental EMS provides the framework.

ISO 14001:2004 is a tool that can be used to meet **internal objectives** such as providing assurance to management that it is in control of the organizational processes and activities having an impact on the environment and assuring employees that they are working for an environmentally responsible organization.

ISO 14001:2004 is a tool that can also be used to meet **external objectives**, such as:

- Providing assurance on environmental issues to external stakeholders (e.g., customers, the community, and regulatory agencies).
- Complying with environmental regulations.
- Supporting the organization's claims and communication about its own environmental policies, plans, and actions.

- Providing a framework for demonstrating conformity via suppliers' declarations of conformity, assessment of conformity by an external stakeholder (e.g., a business client), and for certification of conformity by an independent certification body.

The benefits of using ISO 14001:2004 can include:

- Reduced cost of waste management
- Savings in consumption of energy and materials
- Lower distribution costs
- Improved corporate image among regulators, customers, and the public

(D) ISO 14004:2004 ISO 14004:2004 provides general guidelines on the elements of an EMS and its implementation and discusses principal issues involved.

WHAT ARE THE DIFFERENCES BETWEEN ISO 14001 AND ISO 14004 STANDARDS?

- The ISO 14001:2004 standard specifies the **requirements** for an EMS. An objective audit is needed to demonstrate that the EMS is operating effectively in conformity to the standard.
- The ISO 14004:2004 standard provides general **guidelines** on principles, systems, and support techniques.
- ISO 14004 complements ISO 14001 by providing additional guidance and useful explanations.

(E) Other ISO Standards Other ISO standards related to environmental management include those listed next.

- ISO 14006:2011 provides guidelines for incorporating ecodesign.
- ISO 14031 provides guidance on how an organization can evaluate its environmental performance by selecting suitable performance indicators for internal and external reporting.
- ISO 14040 deals with life cycle analysis.
- ISO 14063 deals with environmental communication for companies to make the important link to external stakeholders.
- ISO 14064:2006 deals with quantification and reporting of greenhouse gas emissions and removals.

(iii) ISO 17021 — Conformity Assessment

The ISO/IEC 17021 standards are equally useful for auditing of the EMS and the QMS. The standards provide guidance on principles of auditing, managing audit programs, the conduct of audits, and the competence of auditors. It is widely used in global markets to establish confidence between business partners and between organizations and their customers, to qualify suppliers in supply chains, and as a requirement to tender for procurement contracts. Examples of ISO standards that received conformity assessments include ISO 9001 (quality management), ISO 14001 (environmental management), and ISO 22000 (food safety management).

(iv) ISO 21500:2012 — Project Management

The ISO 21500:2012 standard provides guidance for project management that can be used by any type of organization, including public, private, or community organizations, and for any type of project, irrespective of complexity, size, or duration.

ISO 21500:2012 provides high-level descriptions of concepts and processes that are considered to form good practice in project management. Projects are placed in the context of programs and project portfolios without detailed guidance on the management of programs and portfolios. Topics pertaining to general management are addressed only within the context of project management.

Examples of benefits of the ISO 21500 standard are listed next.

- Facilitates efficient tendering processes through the use of consistent project management terminology
- Enables the flexibility of project management employees and their ability to work on international projects
- Provides universal project management principles and processes
- Encourages transfer of knowledge between projects and organizations for improved project delivery and business results

(v) ISO 22000:2005 — Food Safety Management Systems

ISO 22000:2005 specifies requirements for a food safety management system where an organization in the food chain needs to demonstrate its ability to control food safety hazards in order to ensure that food is safe at the time of human consumption. This standard is applicable to all organizations, regardless of size, that are involved in any aspects of the food chain and want to implement systems that consistently provide safe products. The means of meeting any requirements of ISO 22000:2005 can be accomplished through the use of internal and/or external resources. This standard requires an organization to meet all applicable food safety–related statutory and regulatory requirements through its management system. In order to comply with the management system, an organization should seek certification or registration of its food safety management system by an external organization, make a self-assessment, or make a self-declaration of conformity to ISO 22000:2005.

(vi) ISO 22301 — Business Continuity Management

The ISO 22301 standard focuses on business continuity management systems and requirements in order to prepare for, protect against, and reduce the likelihood of occurrence of disasters or disruptive incidents (i.e., man-made or natural). The goal is to respond to and recover from disasters and incidents and to improve business continuity capabilities. Organizations will be able to obtain certification to ISO 22301 similar to other certifiable standards, such as ISO 9000, 14000, 27001, and 28000.

(vii) ISO 26000 — Social Responsibility

The ISO 26000 standard provides guidelines for social responsibility. The goal is to encourage voluntary commitment by business organizations to social responsibility with common guidance on concepts, definitions, and methods of evaluation. It is not a management system standard, and it is not intended or appropriate for certification purposes or regulatory or contractual use.

As ISO 26000 does not contain certification requirements, any such certification would be a misrepresentation and would not be a demonstration of conformity with this international standard.

The ISO 26000 standard provides guidance rather than requirements, so it cannot be certified to (unlike some other well-known ISO standards). Instead, ISO 26000 helps clarify what social responsibility is, helps organizations translate principles into effective actions, and shares best practices relating to global social responsibility. It is aimed at all types of organizations regardless of their activity, size, or location. In applying ISO 26000, it is advisable that an organization take into consideration societal, environmental, legal, cultural, political, and organizational diversity as well as differences in economic conditions, while being consistent with international norms of behavior.

The two goals of ISO 26000 are to encourage voluntary commitment by all organizations to social responsibility with common guidance on concepts, definitions, and methods of evaluation; and to act in an ethical and transparent way that contributes to the health and welfare of society.

Six core subjects and issues are addressed in this standard:

1. Human rights (e.g., due diligence, discrimination and vulnerable groups, and resolving grievances)
2. Labor practices (e.g., health and safety at work, social dialogue, human development and training, and employment)
3. The environment (e.g., preventing pollution, sustainable resource use, and handling climate change)
4. Fair operating practices (e.g., anticorruption, fair competition, promoting social responsibility in the value chain, and respect for property rights)
5. Consumer issues (e.g., fair marketing practices, providing consumer service and support, fair contractual practices, consumer data protection and privacy, and access to essential services)
6. Community involvement and development (e.g., skills development, health, wealth and income creation, social investment, technology development and access, and education and culture)

(viii) ISO/IEC 27001:2005 — Information Technology Security Techniques—Requirements of Information Security Management Systems

The ISO/IEC 27001:2005 standard covers all types of organizations (e.g., commercial enterprises, government agencies, and not-for-profit organizations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. This standard uses the PDCA cycle framework.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including:

- Use within organizations to formulate security requirements and objectives.

- Use within organizations as a way to ensure that security risks are cost effectively managed.
- Use within organizations to ensure compliance with laws and regulations.
- Use within organizations as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met.
- Definition of new information security management processes.
- Identification and clarification of existing information security management processes.
- Use by organization management to determine the status of information security management activities.
- Use by internal and external auditors of organizations to determine the degree of compliance with the policies, directives, and standards adopted by an organization.
- Use by organizations to provide relevant information about information security policies, directives, standards, and procedures to trading partners and other organizations with which they interact for operational or commercial reasons.
- Implementation of business-enabling information security.
- Use by organizations to provide relevant information about information security to customers.

(ix) ISO/IEC 27002:2005 — Information Technology Security Techniques—Code of Practice for Information Security Management

The ISO/IEC 27002:2005 standard (previously known as the ISO/IEC 17799 standard) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It addresses IT security techniques and codes of practice for information security management. The objectives outlined here provide general guidance on the commonly accepted goals of information security management. This standard contains best practices of control objectives and controls in these areas of information security management:

- Security policy
- Organization of information security
- Asset management
- HR security
- Physical and environmental security
- Communications and operations management
- Access control
- Information system acquisitions, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

The control objectives and controls just listed are intended to be implemented to meet the requirements identified by a risk assessment. They are intended as a common basis and a set of practical

guidelines for developing organizational security standards and effective security management practices and to help build confidence in interorganizational activities.

(x) ISO 28000:2007 — Security Management Systems for the Supply Chain

The ISO 28000:2007 standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Managers responsible for selecting suppliers for purchasing decisions can refer to ISO 9001 for the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain. Some examples of risks in the supply chain include piracy, fraud, and terrorism.

ISO 28000:2007 is applicable to all sizes of organizations, from small to multinational, in manufacturing (including software and hardware), service, storage, or transportation at any stage of the production or supply chain that wish to:

- Establish, implement, maintain and improve a security management system.
- Ensure conformance with stated security management policy.
- Demonstrate such conformance to others.
- Seek certification/registration of its security management system by an accredited third-party certification body. Organizations that choose third-party certification can further demonstrate that they are contributing significantly to supply chain security.
- Alternately, make a self-determination and self-declaration of conformance with ISO 28000:2007.

It is not the intention of ISO 28000:2007 to require duplicative demonstration of conformance.

(xi) ISO 31000:2009 — Risk Management

The ISO 31000:2009 standard focuses on risk management. It sets out principles, a framework, and a process for the management of risk that is applicable to any type of organization in the public or private sector. It does not mandate a one-size-fits-all approach but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization. Risks affecting organizations may have consequences in terms of societal, environmental, technological, safety, and security outcomes; commercial, financial, and economic disciplines; as well as social, cultural, and political reputation impacts. The standard also addresses crisis management, earthquakes, floods, storms, and hurricanes.

Using ISO 31000:2009 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment. The standard can be applied to any organization, regardless of size, activity, or sector. However, the standard cannot be used for certification purposes, but it does provide guidance for internal or external audit programs. Organizations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance.

The ISO/IEC 31010:2009 standard focuses on risk assessment, which helps decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. The standard focuses on risk assessment concepts, processes, and the selection of risk assessment techniques. The standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences, and is not intended for the purpose of certification.

(xii) ISO 50001:2011 — Energy Management

The ISO 50001:2011 standard focuses on using energy efficiently; it helps organizations save money, conserve resources, and tackle climate change. This standard supports organizations in all sectors to use energy more efficiently, through the development of an energy management system. ISO 50001:2011 is based on the management system model of continual improvement also used for the well-known standards such as ISO 9001, ISO 14001, and ISO 27001 (i.e., through PDCA framework). The model makes it easier for organizations to integrate energy management system into their overall efforts to improve quality and EMS.

The ISO 50001:2011 standard provides a framework of requirements for organizations to:

- Develop a policy for more efficient use of energy.
- Establish targets and objectives to meet the policy.
- Use data to better understand and make decisions about energy use.
- Measure the results.
- Review how well the policy works.
- Continually improve energy management.

(xiii) Other ISO Standards Related to Information Technology

Several ISO standards exist to support IT systems and software testing; these standards are discussed next.

The **ISO 15026** standard addresses software assurance in terms of managing risks and ensuring safety, security, and dependability within the context of system and software life cycles.

The **ISO/IEC 15026-3:2011** standard is applicable to systems and software and is intended for use by:

- Definers of integrity levels, such as industry and professional organizations, standards organizations, and government agencies.
- Users of integrity levels, such as developers and maintainers, suppliers and acquirers, users, and assessors of systems or software, and for the administrative and technical support of systems and/or software products.

The **ISO 17025** standard addresses independent testing of software using either the white box testing method or black box testing method.

The **ISO/IEC 17205:2005** standard specifies the general requirements for the competence to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, nonstandard methods, and laboratory-developed methods.

The **ISO/IEC 27003:2010** standard deals with IT security techniques regarding system implementation guidance in accordance with ISO/IEC 27001:2005 standard.

The **ISO/IEC 27004:2009** standard deals with IT security techniques regarding measurement of controls in accordance with the ISO/IEC 27001:2005 standard.

The **ISO/IEC 27005:2011** standard deals with IT security techniques regarding risk management in accordance with the ISO/IEC 27001:2005 standard.

The **ISO/IEC 27007:2011** standard deals with IT security techniques regarding systems auditing in accordance with the ISO 19011 standard.

The **ISO /IEC 90003:2004 standard** deals with software engineering guidelines for the application of ISO 9001:2000 to computer software. This standard provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation, and maintenance of computer software and related support services. This standard does not add to or otherwise change the requirements of ISO 9001:2000. These guidelines are not intended to be used as assessment criteria in QMS registration or certification.

The application of ISO/IEC 90003:2004 is appropriate to software that is:

- Part of a commercial contract with another organization.
- Available for a specific market sector.
- Used to support the processes of an organization.
- Embedded in a hardware product.
- Related to software services.

3.9 Outsourcing Business Processes

The ability to contract for business or technology services typically enables an organization to offer its customers enhanced services without the various expenses involved in owning the required technology or maintaining the human capital required to deploy and operate it. In many situations, outsourcing offers the organization a cost-effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with IT or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain. Because the functions are performed by an organization outside the institution, the risks may be realized in a different manner than if the functions were inside the organization; as a result, controls designed to monitor such risks are needed.

(a) Scope of Outsourcing

Outsourcing means that an organization goes "outside" for the knowledge and experience required to do a specific job. In simpler terms, it means subcontracting or farming out for business functions, systems, and services. The scope of outsourcing includes HR, tax, legal, help-desk services, technical support, telecommunications and network facilities (computer center) management, disaster recovery services, education and training, ongoing hardware maintenance, data

center design and construction, equipment relocation services, systems integration, application development and maintenance, and other services. The scope is broad and could include all or part of any function, service, process, or system operation.

WHICH SOURCING IS WHAT?

- **Outsourcing** is acquiring noncore products or services from external sources.
- **Insourcing** is keeping core products or services in-house.
- **Cosourcing** is having one or two suppliers for an item. Sometimes one supplier works as a backup for the other.
- **Multiple sourcing** is more common in the supply-chain environment where there are several suppliers in the chain. However, having too many suppliers is not good due to problems in communication and coordination, which is in conflict with the goal of reducing the supply base. A few strong and stable suppliers with long-term commitments are better than many weak and unstable suppliers with short-term commitments.
- **Offshoring** is moving a business function or process to a foreign country but retaining control of it in the home country.
- **Nearshoring** is choosing an outsource provider located either in the home country or in a nearby foreign country.
- **Backsourcing** is the return of a business activity to the original firm in the home country.

Examples of IT operations frequently outsourced by financial organizations include:

- The origination, processing, and settlement of payments and financial transactions
- Information processing related to customer account creation and maintenance
- Other information and transaction processing activities that support critical banking functions, such as loan processing, deposit processing, fiduciary and trading activities
- Security monitoring and testing
- System development and maintenance
- Network operations
- Help-desk operations
- Call centers

(b) Reasons for Outsourcing

Management may choose to outsource business operations and functions for various reasons. These include:

- Gain operational or financial efficiencies.
- Increase management focus on core business functions.
- Refocus limited internal resources on core functions.
- Obtain specialized expertise.

- Increase availability of services.
- Accelerate delivery of products or services through new delivery channels.
- Increase ability to acquire and support current technology and avoid obsolescence.
- Conserve capital for other business ventures.

Outsourcing of business or technology-related services may improve quality, reduce costs, strengthen controls, and achieve any of the objectives listed previously. Ultimately, the decision to outsource should fit into the organization's overall strategic plan and corporate objectives.

Before considering the outsourcing of significant functions, an organization's directors and senior management should ensure that such an action is consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria. The degree of oversight and review of outsourced activities will depend on the criticality of the service, process, or system to the organization's operation as well as quality of service and quality of protection.

(c) Risks in Outsourcing

Organizations should have a comprehensive outsourcing risk management process to govern their business or technology service provider relationships. The process should include risk assessment, selection of service providers, contract review, and monitoring of service providers. Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the organization were conducting the activities in-house.

According to neoIT at www.neoIT.com, offshore outsourcing comes with risk, including cultural compatibility, legal framework, technical infrastructure, geopolitical risks, and security and privacy risks. Security concerns over the IT outsourced vendor include:

- **Business continuity and disaster recovery**, which includes risk assessments, restoration process, testing of backup systems, audits, ongoing monitoring, managing the alternate site, key resources, and postdisaster communication
- **Information protection**, which includes vulnerability assessment and penetration studies (technical and nontechnical), data access, data audits, data security, data transmission, data storage, and virus management
- **Data backup and recovery**, which includes scheduled backups, data recovery, nonstorage of production code and data in an offshore location, and disposal of sensitive data
- **Insurance coverage**, which includes protection over buildings, equipment, personnel, and electronic information
- **Intellectual property rights protection**, which includes agreements, country laws, data security, physical security, legal obligations, compliance to international security and data privacy standards (e.g., European Union, OECD, ISO 27002, Safe Harbor, ITIL, and COBIT), logging and auditing, employee contract, and security management training
- **Network security**, which includes dedicated infrastructure, network security, and network device security
- **Personnel security**, which includes background checks, reference checks, integrity checks, nondisclosure and confidentiality agreements, Internet usage, suppliers' access to hardware, usage of mobile commuting, and housekeeping

- **Physical security**, which includes access control, limited access, camera surveillance, and fire safety

(d) Benefits of Outsourcing

Organizations turn to outsourcing to improve performance (system and people) and to reduce operating costs. On the positive side, outsourcing offers solutions when there is a shortage of in-house skills, when a high-risk and high-overhead project needs to be managed, and when there is an unacceptable lead time to complete a project using company personnel.

The benefits from outsourcing usually focus on performance improvements and/or cost reductions. Another benefit is that it allows internal management's time and resources to be devoted more to the core business and the company's future. Outsourcing prevents hiring additional employees to meet temporary needs. However, outsourcing does not mean surrendering control and internal management responsibility of subcontracted functions and projects to outside vendors.

Some of the organization's IT employees could work for the outsourcing vendor. The key point here is to monitor the performance of the outsourced vendor during the contract period. Selection of an outsourcing vendor is no different from selecting other types of vendors. Selection factors such as vendor proximity, attitude of the vendor's personnel, vendor's reputation and knowledge, and the vendor's financial condition and management's integrity are important to consider.

The fixed-price-type service contract is best for the user organization because the amount is known in advance. However, the fixed-price contract may not be feasible in all situations, especially when cost variables are uncertain and vendors may overbid because of perceived risk and because they have never done this kind of work before. An alternative is incentive contract, where attainable targets are communicated to the contractor and incentive arrangements are designed to motivate contractor efforts that might not otherwise be emphasized and to discourage contractor inefficiency and waste. Another type of contract is share-in-savings arrangement, which includes not only sharing in costs and savings but also providing training and education to the supplier.

The contract should spell out vendor performance-level guarantees, the remedies for nonperformance, and the right-to-audit clause. Contractual risks can be addressed or mitigated through terms and conditions, vendor certifications, evaluation factors for award, and risk mitigation requirements included in the statement of work (SOW).

From the economics point of view, the outsourcing approach provides an option to buy IT or business services from outsiders rather than from the organization's IT or other departments. Users can perform make-or-buy analysis.

(e) Vendor Governance

Vendor governance requires a vendor to establish written policies, procedures, standards, and guidelines regarding how to deal with its customers or clients in a professional and businesslike manner. It also requires establishing an oversight mechanism and implementing industry best practices. Customer (user) organizations should consider the next criteria when selecting potential hardware, software, consulting, or contracting vendors.

- Experience in producing or delivering high-quality security products and services on-time and all the time

- Track record in responding to security flaws in vendor products, project management skills, and cost and budget controls
- Methods to handle software and hardware maintenance, end-user support, and maintenance agreements
- Vendor's long-term financial, operational, technical, and strategic viability
- Adherence to rules of engagement during contractual agreements, procurement processes, and product/service testing

(f) Service-Level Agreements

Contractual agreements in procurement processes for outsourced vendors should include a service-level agreement (SLA). For example, the SLA represents the understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud subscriber. The overall scope of service contract or service agreement includes the SLA, licensing of services, criteria for acceptable use, service suspension and termination, liabilities, guarantees, privacy policy, and modifications to the terms of service.

An SLA is an effective way for computer center management to improve the quality of computing services to system users. The computer center management must define a set of user service levels or service objectives that describe application systems, transaction volume, processing windows, online system response times, and batch job turnaround times. Without well-defined service levels to monitor against actual performance determined in the resource utilization function, a computer system's capacity limit is difficult to identify.

Without service levels, the computer center management will consider computer capacity at its limit when users begin to complain about computer performance. By monitoring performance against service levels, computer center management can identify approaching problems in meeting service objectives. In order to achieve these goals, computer center management needs to develop service-level objectives for internal use.

(i) Areas Needing Service Levels

Some examples of IT areas requiring service level objectives are listed next.

- System capacity during peak hours in terms of average central processing unit (CPU) usage, average demand paging rate, and maximum channel activity
- Number of online users, number of online transactions per minute, and number of batch jobs per hour
- Online system average response time in seconds by application
- Percentage of time the online system is available
- Turnaround time for test and production batch jobs processed under each job class by application

For each of these objectives, a range of minimum and maximum numbers should be identified. The rationale behind developing service-level objectives internally first is that they provide a basis for negotiating SLAs with the user community.

(ii) Performance Metrics for Service Levels

After developing service-level objectives internally, the IT management is ready to negotiate with each business user to develop formal SLAs in terms of performance metrics. Some examples of these metrics are listed next.

- Number of complaints received from system users for each application system
- Average response times for each online application system
- Turnaround times for each batch job by application system
- System availability time (system uptime) by each application system
- Accuracy limits in terms of number of errors by cause for each application system
- Number of job reruns by each application system
- Number of transactions to be processed during peak hours in each application system
- Number of production problems by application system per week
- Computer report delivery times by application system
- Plan for reporting service-level problems
- Action priorities if services cannot be delivered
- Scheduled meetings to discuss service levels between end users and computer center management
- Number of job reruns and time lost due to job reruns
- Number of abnormal terminations by application program per operating shift

It is important to remember that these SLAs are not static. They require adjustments and refinements periodically, such as at least once a year or preferably when renegotiating the agreement with customers (users).

(g) Third-Party Organizations

Third parties include external organizations, such as business partnerships, joint ventures, licensing agreements, outsourcing arrangements, and supply chain exchanges (with acquirers, integrators, and suppliers). Note that there could be more than one supplier in outsourcing arrangements or supply chain exchanges. External organizations operate external systems to provide the needed software products and support services to internal user organizations.

The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. Some of these challenges are listed next.

- Defining the types of external services provided to the organization
- Describing how the external services are protected in accordance with the security requirements of the organization
- Obtaining the necessary assurances that the risk to organizational operations and assets, individuals, and other organizations arising from the use of the external services is acceptable

The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust that the organization places in the external service provider. This leads to three security issues that must be addressed: (1) level of trust, (2) level of control, and (3) chain of trust.

In some cases, the **level of trust** is based on the amount of direct control the organization is able to exert on the external service provider with regard to employment of security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls.

The **level of control** is usually established by the terms and conditions of the contract or SLA with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a standard contract or SLA to obtain commodity services, such as commercial telecommunications services).

In other cases, the level of trust is based on factors that convince the user organization that the requisite security controls have been employed and that a determination of control effectiveness exists. For example, a separately authorized external information system service provided to an organization through a well-established line of business relationship may provide a **degree of trust** in the external service within the tolerable risk range of management.

Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with the user organization's management. Organizations require that an appropriate **chain of trust** be established with external service providers when dealing with the many issues associated with information system security. A chain of trust requires that the organization establish and retain a **level of confidence** that each participating service provider in the potentially complex consumer–provider relationship provides adequate protection for the services rendered to the organization.

The chain of trust can be complicated due to the number of entities participating in the consumer–provider relationship and the type of relationship between the parties (i.e., long or short supply chain). External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to place significant trust in the service provider, not due to any inherent untrustworthiness on the provider's part but due to the intrinsic level of risk in the service.

Where a significant level of trust cannot be established in the external services and/or service providers, the user organization (1) employs compensating security controls, (2) accepts a greater degree of risk, (3) does not obtain the service, or (4) performs business operations with reduced levels of functionality or no functionality at all.

The chain of trust is related to the level of confidence, level of trust, level of control, and degree of trust in that order, as shown:

Level of Confidence → Level of Trust → Level of Control → Degree of Trust

(h) Managing Third-Party Organizations

Managing third-party organizations and their systems is a difficult and complicated task because they are not under the direct control of the user organizations. Managing requires four steps:

1. Needs assessment (i.e., initial risk assessment and security requirements).
2. Service contract (i.e., request for information/request for proposal/request for quotation, contract negotiations, SLA, and due diligence). Before finalizing a service contract, a due diligence review should be performed, and a request for proposal document, a statement of work (SOW) document, and an SLA document should be prepared in that order.
3. Security appraisal (i.e., system vulnerabilities, software patches and upgrades, security incidents, software disposal/decommissioning, and change management).
4. Third-party audit (i.e., review of operational systems of external service providers).

3.10 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. The relationship between organizational structure and technology suggests that in an organization using mass production technology (e.g., automobile manufacturing), the **best** structure would be:

a. Organic, emphasizing loose controls and flexibility.

b. Matrix, in which individuals report to both product and functional area managers.

c. Mechanistic, that is, highly formalized, with tight controls.

d. Integrated, emphasizing cooperation among departments.

2. Routine tasks, which have few exceptions and problems that are easy to analyze, are conducive to:

a. Formalized structure, where procedure manuals and job descriptions are common.

b. Decentralized decision making, where decisions are pushed downward in the organization.

c. Organic structures that emphasize adaptability and flexibility to changing circumstances.

d. High degrees of job satisfaction on the part of employees performing them.

3. Which of the following theories predicts that employee behavior depends on the belief that good performance will be rewarded by continued employment?

a. Equity theory: Employees compare their job inputs and outcomes with those of others and then react to eliminate inequities.

b. Expectation theory: The strength of a tendency to act in a certain way depends on the strength of an expectation that an act will be followed by a given outcome.

c. Goal-setting theory: Specific and difficult goals lead to higher performance.

d. Reinforcement theory: Behavior is a function of its consequences.

4. Which of the following has a flat organizational structure compared to others?

a. Organization A with 11 hierarchical levels.

b. Organization B with 3 hierarchical levels.

c. Organization C with 8 hierarchical levels.

d. Organization D with 6 hierarchical levels.

5. The most fundamental flaw of cost-plus pricing is that it:

a. Fails to account for competition.

b. Ignores demand.

c. Ignores industry-wide standard markup policies.

d. Places too much emphasis on competition.

6. "Selling price = Unit cost + Desired profit" represents which of the following pricing approaches?

a. Profit maximization

b. Demand-based pricing

c. Target return pricing

d. Standard markup

7. Choosing vendors based solely on which of the following factors is detrimental to the long-term success of a buying firm?

a. Quality

b. Service

c. Price

d. Delivery

8. Supplier audits are an important first step in:

a. Supplier certification.

b. Supplier relationships.

c. Supplier partnerships.

d. Strategic partnerships.

9. Customers in which of the following phases of the product life cycle are called laggards?

a. Introduction

b. Growth

c. Maturity

d. Decline

10. Few competitors exist in which phase of the product life cycle?

a. Introduction

b. Growth

c. Maturity

d. Decline

11. Regarding the theory of constraints in operations, which of the following does **not** describe a bottleneck situation appropriately?

a. A machine exists where jobs are processed at a slower rate than they are demanded.

b. A work center exists where jobs are processed at a slower rate than they are demanded.

c. An employee's skill levels are more than needed for a specific job but less than needed for any general job.

d. The demand for a company's product exceeds its ability to produce that product.

12. Regarding production process flows, which of the following is **not** a part of the levers for managing throughput of a process?

a. Decrease resource idleness

b. Increase effective capacity

c. Reduce setup resources

d. Decrease theoretical capacity

13. Which of the following inventory items would be the **most** frequently reviewed in an ABC inventory control system?

a. Expensive, frequently used, high stock-out cost items with short lead times

b. Expensive, frequently used, low stock-out cost items with long lead times

c. Inexpensive, frequently used, high stock-out cost items with long lead times

d. Expensive, frequently used, high stock-out cost items with long lead times

14. What are the three factors a manager should consider in controlling stock-outs?

a. Holding costs, quality costs, and physical inventories

b. Economic order quantity, annual demand, and quality costs

c. Time needed for delivery, rate of inventory usage, and safety stock

d. Economic order quantity, production bottlenecks, and safety stock

15. Reordering of specific items from vendors should be based on:

a. Computations on the basis of economic order quantities.

b. Demand forecasting based on early orders for the items.

c. Market demographics.

d. Vendor quantity discounts and warehouse space.

16. A risk associated with just-in-time (JIT) production is the:

a. Increased potential for early obsolescence of inventories of finished goods.

b. High cost of material handling equipment.

c. Potential for significant costs associated with reworking defective components.

d. Critical dependency on a few vendors.

17. With regard to inventory management, an increase in the frequency of ordering will normally:

a. Reduce the total ordering costs.

b. Have no impact on total ordering costs.

c. Reduce total carrying costs.

d. Have no impact of total carrying costs.

18. Which of the following represents an integration of diverse technologies such as point-of-sale terminals, personal identification numbers, and automated teller machines?

a. Electronic data interchange systems

b. Electronic funds transfer systems

c. Intranet systems

d. Extranet systems

19. Stock brokers/dealers and stock markets employ which of the following electronic commerce models?

a. Consumer-to-business (C2B)

b. Business-to-consumer (B2C)

c. Business-to-business (B2B)

d. Exchange-to-exchange (E2E)

20. In which of the following phases of business development life cycle will both outputs and employment be declining?

a. Peak

b. Recession

c. Trough

d. Recovery

21. In business activity, both seasonal variations and secular trends are due to which of the following?

a. Cyclical fluctuations

b. Noncyclical fluctuations

c. Business expansions

d. Business contractions

22. The ISO 14000 standard focuses on environmental management system and the ISO 14001 standard focuses on the framework for implementing environmental strategies. Which of the following is the scope of the ISO 14001 standard?

a. Minimize waste in products.

b. Minimize redesign of products.

c. Conduct environmental audit.

d. Prevent pollution.

23. The ISO 22301 standard focuses on which of the following subjects?

a. Business continuity management systems and requirements

b. System and software life cycles

c. Code of practice for information security management

d. Independent software testing

24. Which of the following scope items for an outsourced vendor takes on a significant dimension in a supply-chain environment?

a. Liabilities and guarantees

b. Well-defined service levels

c. Licensing of services and products

d. Changes to terms and conditions of services

25. When managing a third-party organization such as an outsourcing vendor, which of the following is **not** applicable?

a. Due diligence review

b. Rules of engagement

c. Rules of behavior

d. Contractual agreement

DOMAIN 4

Communication (5–10%)

4.1 Communication Skills

Topics such as communication process, barriers to communication, organizational dynamics, and impact of computerization on communication are discussed in this section.

(a) Communication Process

One thing that is common to all four functions of management (i.e., planning, organizing, directing, and controlling) is communication. Surveys have shown that 80% of a manager's time is spent on communication and 20% on other activities. Management scholar Keith Davis[1] has defined communications as "the transfer of information and understanding from one person to another person." Communication involves two or more people. The effectiveness of organizational communication can be increased with clear verbal and written messages with little or no noise. Kreitner[2] describes communication as a chain made up of identifiable links—sender, encoding, medium, decoding, receiver, and feedback (see Exhibit 4.1). The communication chain is only as strong as its weakest link.

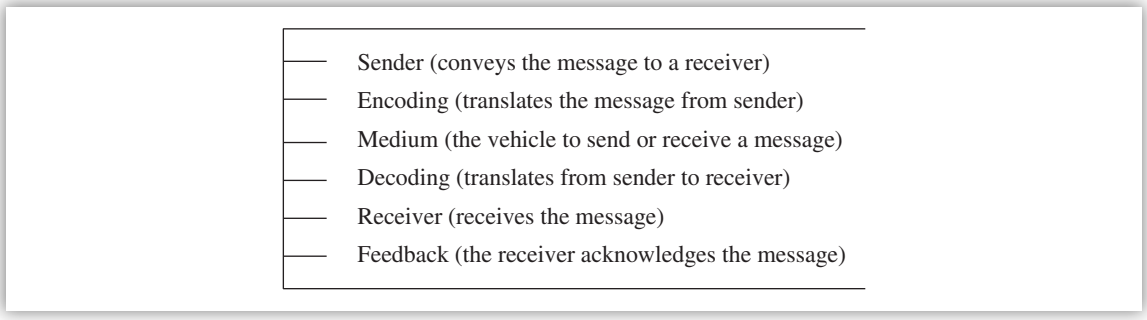


EXHIBIT 4.1 Links in the Communication Chain

[1] Keith Davis, "Grapevine Communication among Lower and Middle Managers," *Personnel Journal* (April 1969).
[2] Robert Kreitner, *Management* (Boston, MA: Houghton Mifflin), 2004.

(i) Sender

The sender is an individual or a group of people whose goal is to convey or transmit the message to a receiver in the best possible media and in the fastest way.

(ii) Encoding

The objective of encoding is to translate internal thought patterns into a language or code that the intended receiver of the message will be able to understand. Words (written or oral), numbers, gestures, or other symbols are used in encoding. The purpose of the message affects the medium of encoding. For example, if a manager were proposing a new employee benefit plan, which is a sensitive program, a meeting with emotional appeal and gestures would have a bigger impact than a normal written (cold) report. A meeting conveys personal interest and empathy, unlike a report.

(iii) Medium

Many types of media exist to send and receive a message, including, face-to-face communications, telephone calls, regular meetings and electronic meetings (video-conferencing), memos, letters, reports, facsimiles, bulletin boards, newsletters, and others. Each media type varies in richness from high rich to low rich. Media richness is described as the capacity of a given medium to convey information properly and promote learning. *The goal is to match media richness with the situation. Otherwise, mismatching occurs, which can lead to confusion and embarrassment.*

Examples of high-rich media include face-to-face conversation, telephone, or video-conferencing, since they provide multiple information cues (e.g., message content, tone of voice, facial expressions), facilitate immediate feedback, and are personal in focus. High-rich media is good for discussing nonroutine issues and problems.

Examples of low-rich or lean media include bulletin boards, reports, memos, e-mail, text messages and letters. These media provide a single cue, do not facilitate immediate feedback, and are impersonal. Low-rich media is good for discussing routine problems.

Example

To quash a rumor of bad news about a large company, senior management should issue a memorandum or e-mail to each employee since it conveys the same message in a timely manner. Meetings of all employees should not be used since such meetings are logistically difficult to assemble unless the company is very small. A front-page message in the monthly company newsletter is not timely as the newsletter comes out only once a month.

(iv) Decoding

Decoding is the translation of the transmitted message from the sender's language and terminology to that of the receiver's. Effective decoding requires that these messages be the same between the sender and the receiver. The receiver's willingness to receive the message is a primary criterion for successful decoding.

(v) Receiver

The receiver is an individual or a group of people whose goal is to acknowledge and receive the intended message sent by a sender. The receiver will take an action based on the message received.

(vi) Feedback

The communication process is not complete until the receiver acknowledges the message (via verbal or nonverbal feedback) to the sender. Without feedback, the sender is not sure whether the receiver has received the message. Feedback affects follow-up: If the receiver does not understand the message, follow-up meetings should be scheduled.

(vii) Noise

Noise is not part of the chainlike communication process. It is any interference with the normal flow of understanding of a message from one person to another. Examples of noise include misperception, illegible print, speech impairment, and garbled computer data transmission. Understanding has an inverse relationship with noise—the higher the noise, the less the understanding. For effective communication to take place between and among people, we all need to identify the sources of noise and reduce it. Greater amounts of noise in communication not only waste resources (time and money) but also create frustration between the sender and the receiver.

Example

A manager found that instructions given to a subordinate were not followed. A review of the cause of the failure revealed that the manager was interrupted by several telephone calls while issuing the instructions. In terms of problems in the communication chain, the interruptions are noise.

(viii) Perception

Perception is a process of giving meaning to one's environment, and is a vital link in the communication process. It consists of three subprocesses: selectivity, organization, and interpretation. Selectivity is sensory screening and a sorting out process. Organization is mentally creating meaningful patterns from disorganized thoughts. Interpretation is how people understand a message, which is often different for different people.

(ix) The Grapevine

A grapevine is the unofficial and informal communication system. It sometimes conflicts with the formal system; at other times, it complements and reinforces the formal system. The grapevine will remain in organizations as long as people are working in a group environment. It has both positive and negative sides. From a positive side, grapevine communication can help management learn how employees truly feel about policies, procedures, and programs—a type of feedback mechanism. A negative consequence to the grapevine is rumors.

(b) Barriers to Communication

It is false to assume that if people can talk, they can communicate. Talking is different from communicating. Many barriers exist between all people, which make communications much more difficult than most people seem to realize. The auditor needs to know all the barriers that exist that can block effective communication. The negative effects of roadblocks to communication include diminishing of self-respect in others, triggering defensiveness, resistance, and resentment. Negative effects can also lead to dependency, withdrawal, and feelings of defeat or of inadequacy.

Kreitner[3] describes four types of barriers to communication representing extreme forms of noise: (1) process barriers, (2) physical barriers, (3) semantic barriers, and (4) psychological or social barriers.

Communication barriers = Process → Physical → Semantic → Psychological/Social

The scope of process barriers consists of sender barrier, encoding barrier, medium barrier, decoding barrier, receiver barrier, and feedback barrier—links in the communication chain. The scope of physical barriers includes physical objects blocking the effective communication (e.g., walls, medium). Semantic barriers address the words used in the communication. *An auditor who uses jargon in an audit report is likely to encounter the semantic form of communication barrier. Psychological and social barriers deal with people's backgrounds, perceptions, values, biases, needs, and expectations—all of which differ to varying degrees.*

When someone is experiencing stress, it is good to avoid all roadblocks. If someone is experiencing a strong need or wrestling with a difficult problem, the likelihood of negative impact from roadblocks increases greatly. Robert Bolton[4] presents 13 roadblocks, which can be divided into three major categories: judging, sending solutions, and avoiding the other's concerns.

(i) Judging

Judging involves approving or disapproving of the statements of the other person, and it is the major roadblock for effective communication (see Exhibit 4.2).

EXHIBIT 4.2 Aspects of Judging

Many of us feel we ought to be critical; otherwise, people will never improve. For some people, **criticism** is a way of life. Auditors should be mindful of this because their work can be taken as a criticism of the person who is being audited. **Name-calling** and labeling have negative overtones to both sender and receiver. This is because labeling prevents us from getting to know other individuals and ourselves.

Diagnosing is a form of labeling and occurs when the listener does not listen to the substance of what a person is saying or plays emotional detective, probing for hidden motives, and the like. **Praising**, or expressing positive feelings toward people, is an important element of interpersonal communication. Honest praise is helpful. **Pointing the finger** at others does not improve communication *or* relationships.

(ii) Sending Solutions

Sending solutions to others can be risky. The person receiving the solution can misinterpret or misread the solution as ordering, threatening, moralizing, and advising (see Exhibit 4.3). This can

[3] Ibid.
[4] Robert Bolton, *People Skills* (New York: Simon & Schuster, 1979).

create a roadblock to communication. Sending a solution can compound a problem or create a new problem without resolving the first one.

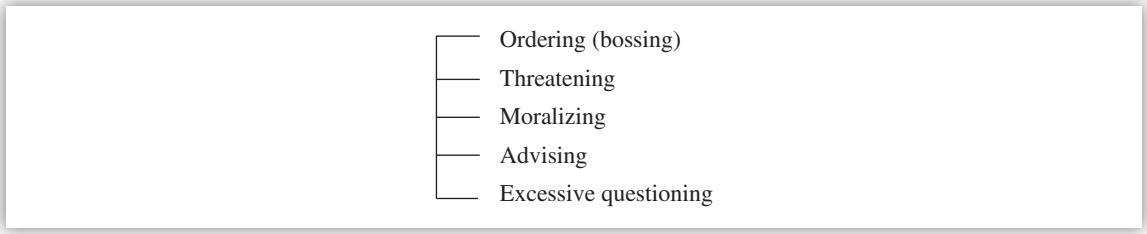


EXHIBIT 4.3 Sending Solutions

An **order** is a solution sent coercively and backed by force. Coercion leads to resistance and resentment. A **threat** is a solution that is sent with an emphasis on the punishment that will be forthcoming if the solution is not implemented.

Moralizing (e.g., "It is the right thing to do") fosters anxiety and invites pretense. **Advice** can be interpreted as a basic insult to the intelligence of the other person. The advisor may not understand the full implications of the problem. Another issue is that many people give advice inappropriately. The advice-giving trap is very tempting and should be avoided whenever possible.

Extensive questioning often derails a conversation. Indirect or incomplete questions often breed defense reactions and resistance. Auditors' actions might be seen as "sending solutions."

(iii) Avoiding the Other's Concerns

Avoiding the other's concerns is another example of a roadblock to communication (see Exhibit 4.4).

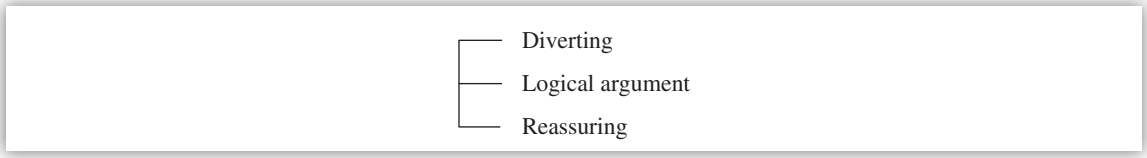


EXHIBIT 4.4 Avoiding the Other's Concerns

Some people **divert** a conversation because they cannot listen effectively or want attention from the speaker. Others divert the conversation to a topic more comfortable for them. When another person is under stress or when there is a conflict between people, there is no place for logical solutions.

Logic focuses on facts, but a stressed person likes to address his or her feelings—the two do not fit. **Reassurance** can drive a wedge between people. Reassurance is a way of seeming to comfort another person while actually doing the opposite. It can be a form of emotional withdrawal. People who like the idea of being helpful but who do not want to experience the emotional demands that go with it often use reassurance.

(iv) Essentials for Effective Communication

After presenting the 13 barriers to communication, Bolton[5] describes three essentials for effective communication: genuineness, nonpossessive love, and empathy.

[5] Ibid.

ESSENTIAL COMMUNICATION DEFINITIONS

- **Genuineness** means being honest and open about one's feelings, needs, and ideas.
- **Nonpossessive love** involves accepting, respecting, and supporting another person in a nonpaternalistic and freeing way.
- **Empathy** refers to the ability to really see and hear another person and understand the person from his or her perspective.

The person who has mastered the skills of communication but lacks genuineness, nonpossessive love, and empathy will find his or her expertise irrelevant or even harmful.

Genuineness means being what one really is without a front or facade. Genuineness is essential to all vital relationships, especially auditor–auditee relationships. It is being honest and open with others.

Other names for **nonpossessive love** are: respect, acceptance, and positive regard toward others. Respect recognizes the sanctity of the other's privacy, supports the other person's self-direction, and respects his or her individuality. Acceptance is an attitude of neutrality toward another person. Every person is in need of acceptance.

SOME GOLDEN RULES FOR ACCEPTANCE

- No one is perfectly accepting.
- Some people tend to be more accepting than others.
- The level of acceptance in a person is constantly shifting.
- Each of us can become more accepting.
- Pseudo-acceptance is harmful to other people.
- Acceptance is not synonymous with approval. It is possible to be accepting and yet still confront the problem at hand.

Acceptance and respect may or may not be accompanied by warmth. Once you accept and respect a person, that person tends to be more at ease around you.

Empathy is simply putting yourself in somebody else's shoes. It is the ability to understand another person in the same way as that person understands him- or herself.

APATHY VERSUS EMPATHY VERSUS SYMPATHY

- Apathy is a lack of feeling or a lack of interest or concern (e.g., "I don't care").
- Empathy involves experiencing the feelings of another person without losing one's own identity (e.g., "Looks like you are feeling down").
- Sympathy is defined as feelings for another person (e.g., "I feel just dreadful for you").

One needs to be careful with empathy because it can be perceived as excessive if a person identifies very closely with another. There must be a balance between detached involvement and attached involvement.

There is more than one way to express attitudes such as genuineness, nonpossessive love, and empathy. The more a person develops communication skills, the greater the number of constructive alternatives that become available to him or her. However, communication skills cannot be a substitute for caring, authenticity, and understanding. As we develop these three skills, we grow into the more communicative person that we can become. Bolton[6] suggests four steps to improved communication:

1. Commitment to use the skills
2. Application of the skills
3. Willingness to accept occasional failures
4. Willingness to keep practicing and improving the skills

It is advisable to practice first in calm settings before trying the skills in more dramatic situations. There is much to gain with training and confidence in handling difficult situations. No skill is a panacea. Occasional failure should be expected. Persistence in the face of occasional failure is a necessity for persons who are committed to developing any skill. It is usually beneficial to tell the people with whom you are dealing that you will be trying to utilize some new approaches to communication, what these approaches will be, and why you are doing it.

(v) Information Communicated by Others

Information can be improperly analyzed and incorrectly interpreted. The causes of poor business decisions can be attributed not only to a lack of information but also to the failure to properly interpret information.

Proper interpretation of information depends largely on the reliability of the source, the manner in which the information is presented, and the personal perception of the person receiving or giving the information.

METHODS OF COMMUNICATION

- Listening
- Writing
- Speaking

Is the source reliable? Unbiased? No source is unimpeachable. The main question is really whether it is the only source. If it is, then the data are as reliable as they can be. If it is not, then a second source should be checked and is likely to produce a different set of data.

Independent sources can be assumed to be unbiased while data from self-interested parties may well be biased. Is the information provided by the source up to date? Is it firsthand or secondhand? Surveys and census data are firsthand; hearsay is secondhand information.

[6] Ibid.

The manner in which information is presented can significantly affect its use. Most information, which has been assembled from statistics, data, and facts, has been "massaged" (assembled in a manner applicable to a particular problem at hand). This is because if 10 people created charts from the same set of statistics, we would have 10 different charts. Each person would massage the information in a different way—yet all the different charts could be correct.

Proper and accurate interpretation also depends on our own abilities of perception. Always keep the original question or problem in mind and pay close attention to details. It is good to view all information with a bit of healthy skepticism because information is not an exact science. *The return on an investment in information is knowledge.*

(vi) Communications and Internal Auditor Applications

When the internal auditor practices the three communication skills (genuineness, nonpossessive love, and empathy), it is easier to agree to disagree with the auditee about audit findings, values, and other issues. The goal is to solve real problems on a win-win basis (i.e., both parties win).

(c) Organizational Dynamics

Organizational dynamics is a combination of individual dynamics, group dynamics, and work-related environmental dynamics.

(i) Individual Dynamics

Individual dynamics deal with how an individual's needs and wants are satisfied at the workplace. Managers should understand Maslow's hierarchy of needs, which help to explain the actions of employees at the workplace.

(ii) Group Dynamics

Group dynamics deal with how group members interact with each other at the workplace and how managers resolve group problems. Each member of the group plays an expected role, and the group has its own biases, values, and beliefs. Another dimension affecting group dynamics is conflicts among departments or functions within an organization.

Communication among groups also affects organizational dynamics. Managers receive and transmit information on the basis of how they relate to themselves and others. According to Joseph Luft and Harry Ingram,[7] managers deal with four levels of communication (known as the Johari Window).

1. **Arena.** All information needed to carry on communication is known by the manager and other individuals.
2. **Blind spot.** The manager does not know information that is known to others.
3. **Facade.** Information is known by the manager and not by others.
4. **Unknown.** Neither the manager nor others are aware of the information each knows.

[7] Joseph Luft and Harry Ingram, *An Introduction to Group Dynamics* (Palo Alto, CA: National Press Books), 1963.

(iii) Work-Related Environmental Dynamics

The environment—physical and social—is part of the situational context of human behavior.[8] We are affected not only by our relationships with others but by the places and spaces in which we interact. The science of transactions between human behavior and the environment is called environmental psychology.

(iv) Environmental Perception

The way we interact with and treat our environment begins with the way we perceive and think about it. People are strongly motivated to make sense of their environment. We collect information so that we can make predictions and behavioral choices. Here we are interested in evaluating the environment's physical features and social climate.

Evaluating an environment from a physical setting involves determining whether it is "good" and whether we "like" it. Evaluative dimensions are affected by culture. The social climate offers three kinds of experiences that can be evaluated: social relationships, personal development, and organizational stability. Individuals generally prefer environments that foster relationships and interactions with others (i.e., social relationships). We also need opportunities for privacy and activity, important aspects of personal development. Organizational stability deals with managing change, which is inevitable. The needs of individuals and groups change over time; some settings can be adjusted for these changes while others resist modification (i.e., they are too stable).

(v) Social Environment

Because we share our environment with other people, much of the environment's impact on us is social. Four special phenomena directly involved with our environment are (1) crowding, (2) privacy, (3) spatial behavior, and (4) territoriality (see Exhibit 4.5).

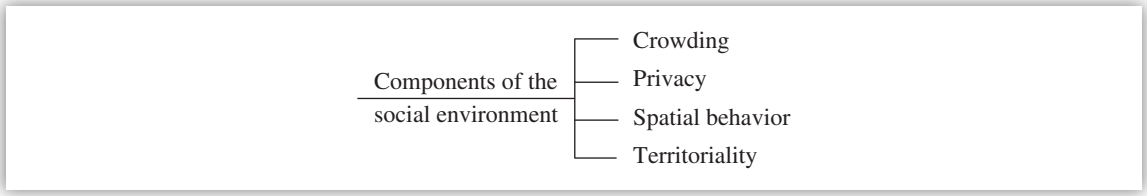


EXHIBIT 4.5 Components of the Social Environment

(A) Crowding Crowding is the subjective judgment that one has insufficient space. Density and the objective condition of too many people within an area usually cause it. Either physical density or social density causes crowding. Physical density involves too little space per person. In contrast, social density involves too many people for a given area. Social density has been found to cause more negative feelings than physical density. The presence of many others involves several potential stressors; insufficient space, distraction, and invasion of privacy. *Auditor's tip:* It is not a good idea to interview or engage in an audit-related communication with an auditee when there are too many people in a given area. It is better to schedule a more private meeting, preferably a face-to-face interview.

(B) Privacy Privacy refers to one's ability to control others' access to oneself. Crowding is experienced when we fail to regulate privacy in our social experience.

[8] Ann L. Weber, *Social Psychology* (New York: HarperCollins, 1992).

CROWDING VERSUS ISOLATED

- When we have more social stimulation than we want, we feel crowded.
- When we have less social attention than we want, we feel isolated.
- Crowding and isolation are problems created when our social environment does not meet our social needs.

To regulate privacy—to get the amount of space we want—we try to adapt to our social conditions by using regulation mechanisms, including nonverbal behaviors, movement, and physical props. Increasing or decreasing eye contact with the other person is an indication of wanting less privacy or more privacy respectively. Privacy is important to one's sense of well-being, affecting personal control and self-efficacy. Invasions of privacy evoke defensive or escape behaviors. *Auditor's tip:* Be mindful of invading the auditee's privacy when communicating during the audit work.

(C) Spatial Behavior The study of spatial behavior is called protemics. Two topics in protemics are zones of interpersonal distance and the maintenance and defense of personal space.

Interpersonal distance deals with zones of interpersonal distance associated with different levels of intimacy and qualities of interaction. Anthropologist Edward T. Hall[9] has identified four zones of distance: (1) intimate, (2) personal, (3) social, and (4) public.

Intimate distance extends from zero to 18 inches from the body. At this distance, people can see great details and speak in low tones and whispers. The *personal distance* zone ranges from 18 inches to 4 feet from the body. It is the appropriate distance for friendly conversation, and voice ranges are normal.

The *social zone* ranges from 4 to 12 feet from the body. Business and formal transactions are most likely to occur within social distance. Props like office desks can be used to keep others at a social distance. High-status persons prefer keeping others farther away and have more control over whether and when others come closer. Voices may be slightly raised to compensate for distance; little detail is visible.

Interaction across 12 or more feet from the body is within the *public zone*. No detail is observable, voices are raised, and nonverbal gestures may be exaggerated. This is the zone for formal addresses and lectures. *Auditor's tip:* A social zone of distance needs to be maintained during the audit, especially between the auditor and the auditee, and a public zone of distance is preferred in audit training classes.

Personal space is an area around individuals as an extension of their bodies. This personal space can be thought of as a portable territory, extended about arm's length in front and to the sides of the body and somewhat less than that distance behind a person. We protect our personal space, control who may enter or approach, and move to adjust to intrusions.

Personal space varies with one's age, gender, and culture. With respect to culture, Mediterraneans have smaller personal space ranges than Americans do, while Northern European cultures have

[9] Edward T. Hall, *The Hidden Dimension: How Cultures Collide* (Garden City, NY: Doubleday, 1996).

larger ranges. These variations suggest that personal space is learned and modified by experience. People discourage and control space invasions with a variety of actions like staring, averting eye contact, shifting, and commenting, or using physical barriers (e.g., placing a newspaper in between). *Auditor's tip:* When auditing a foreign subsidiary, it is good to learn about that country's culture as far as personal space is concerned in order to avoid any discomfort to auditees.

(D) Territoriality Territoriality is personal ownership or control of physical space and objects. Some ethologists have speculated that human aggression is based on territorial instinct. When a student in a classroom carves initials into a desktop, she is marking territory.

(vi) Human Impact on the Environment

Environmental psychology studies environment–behavior transactions, including both environmental impact on humans and human impact on the environment. We confront environmental demands in two ways: by adaptation (i.e., by conforming our behavior to the limits of our spaces) and by adjustment (i.e., by changing our spaces to fit our needs). Here we will focus on work environments. Traditional work environments assembled people and tasks with little concern for enhancing performance or comfort. Modern work designs consider the nature of the work to be done and the needs of the individuals likely to be doing the work.

(d) Impact of Computerization on Communication

Computers and networks have a greater impact on communication, whether it is electronic mail (e-mail), telephone (land, mobile, or cell), fax, personal digital assistants (PDAs), and others. They all increase speed at which the communication traverses between parties. The result is increased efficiency for participants in the communication process. For example, e-mail can be used to submit ideas for a new project under consideration, to request agenda for meetings, and to conduct surveys. A cell phone application can facilitate work collaboration through phones connecting to a computer server and finding relevant information.

Another application is groupware, where it links workgroups across a room or across the globe. A groupware system permits every member to see the schedules, meeting agendas, and share common information. A collaborative system can share information without the constraints of time and space. Examples of applications in the collaborative system include calendar management, video conferencing, group authoring, telecommuting, meetings, and e-mails.

4.2 Stakeholder Relationships

In this section, topics such as handling stakeholders (such as shareholders; investors; creditors; stock markets; investment analysts; employees; labor unions; regulators and government authorities; suppliers; vendors; contractors; and customers) are presented. In addition, dealing with purchasing agents, buyers, or commodity /service experts; marketing and salespeople; and related parties and third parties is highlighted.

(a) Handling Shareholders and Investors

Shareholders are investors (owners) of a company whereas creditors are lenders of money to the company, which is the borrower of money. Equity investors have certain property rights. For

example, an equity share in a publicly traded company can be bought, sold, or transferred. An equity share also entitles the investor to participate in the profits of the corporation, with liability limited to the amount of the investment. In addition, ownership of an equity share provides a right to information about the corporation and a right to influence the corporation, primarily by participation in general shareholder meetings and by voting.

According to Business Roundtable, shareholder value is enhanced when a corporation treats its employees well, serves its customers well, fosters good relationships with suppliers, maintains an effective compliance program and strong corporate governance practices, and has a reputation for civic responsibility.[10]

Business Roundtable suggests these relationships with shareholders and investors:

- Corporations have a responsibility to communicate effectively and candidly with shareholders. The goal of shareholder communication should be to help shareholders understand the business, risk profile, financial condition, and operating performance of the corporation and the board's corporate governance practices.

WHAT ARE THE INITIATIVES OF SHAREHOLDERS AND CORPORATIONS?

Examples of shareholder initiatives include:

- An increase in filing of shareholder lawsuits against directors especially with respect to a buyout offer price
- An increase in shareholder activist groups through organizing and exercising power over company management
- An increase in filing of shareholder resolutions at annual meetings through booklets of shareholder questions

Examples of corporation initiatives include:

- Increasing amounts of full disclosure of information to investors that affects their investment decisions
- Showing full accountability and transparency to shareholders about business activities, financial condition, and tender offers made during mergers and acquisitions
- Avoiding conflict-of-interest situations by board members and executives
- Avoiding the use of insider information for personal gain by board members and executives
- Avoiding personal use of company assets and taking personal loans by directors and executives

- Corporations communicate with investors and other constituencies not only in proxy statements, annual and other reports, and formal shareholder meetings but in many other ways as well. All of these communications should provide consistency, clarity, and candor.
- Corporations should establish effective procedures for shareholders to communicate with the board and for directors to respond to shareholder concerns. The board, or an independent committee such as the corporate governance committee, should establish, oversee, and regularly review and update these procedures as appropriate.

[10] *Principles of Corporate Governance* (Washington, DC: Business Roundtable, 2005), pp. 31–33.

- A corporation's procedures for shareholder communications and its governance practices should be readily available to shareholders. Information about the board's structure and operations, committee composition and responsibilities, corporate governance principles, and code of ethics should be widely disseminated to shareholders.
- The board should be notified of shareholder proposals, and the board or its corporate governance committee should oversee the corporation's response to these proposals.
- Directors should attend the corporation's annual meeting of shareholders, and the corporation should have a policy requiring attendance absent unusual circumstances. Time at the annual meeting should be set aside for shareholders to submit questions and for management or directors to respond to those questions.
- The board should respond appropriately when a director nominee receives a significant "withhold" or "against" vote with respect to his or her election to the board. The corporate governance committee should assess the reasons for the vote and recommend to the board the action to be taken, which should be communicated to the corporation's shareholders.
- In planning communications with shareholders and investors, corporations should consider candor, need for timely disclosure, use of technology, and ultimate goal of shareholder communications (e.g., honest, intelligible, meaningful, timely, and broadly disseminated information).

(b) Handling Creditors

Creditors can provide oversight feedback regarding achievement of an organization's objectives. For example, a bank may request reports on an organization's compliance with certain debt covenants and can recommend performance indicators or other desired targets or controls. Creditors should go beyond the credit rating issued by credit-rating agencies for a company; they should analyze financial statements for off–balance sheet transactions and review annual reports and other documents to get a big picture of the company's products, services, and risk levels.

(c) Dealing with Stock Markets

The U.S. stock markets issued corporate governance rules for listed companies to improve corporate governance practices. They also issued broker-dealer rules to control the behavior of investment analysts. The aim of these rules is to bring integrity to the capital markets and confidence to investors.

Publicly traded companies with common stock issued on the New York Stock Exchange (NYSE), Nasdaq, and American Stock Exchange (Amex) are required to file an annual report containing audited financial statements.

Some examples of the NYSE's rules are listed next.

- Research analysts employed by NYSE members must register with the NYSE and must pass a qualification examination and comply with a continuing education requirement/
- Broker-dealers must disclose the percentage breakdown of their buy, hold, and sell recommendations.
- A firm cannot retaliate against analysts for unfavorable or negative research or ratings.

- Securities analysts are freed from the supervision and control of investment banking management regarding compensation, pending research reports, and the extent of coverage of a company.
- Broker-dealer firms and their analysts must disclose ownership of common shares in the securities of a recommended issuer.
- Each participating investment bank must hire at least three independent securities analysts.

(d) Dealing with Investment Analysts

Investment analysts (also known as research analysts, financial analysts, or securities analysts) consider many factors relevant to an organization's worthiness as an investment opportunity. Investment analysts make buy, hold, or sell recommendations to current or potential investors. During this process, they analyze:

- Management's strategies and objectives.
- Historical financial statements and prospective financial information.
- Actions taken in response to conditions in the economy and marketplace.
- Potential for success in the short and the long term.
- Industry performance and peer group comparisons.

Investment analysts provide insights to a company management on how others perceive the organization's performance (outside-in perspective), risks that may impact the organization, operating or financing strategies that may improve performance, and industry trends.

This information is provided directly in face-to-face meetings of investment analysts and company management or through analyst reports issued to current and potential investors. In either case, company management should consider the observations and insights of investment analysts that may enhance the organization's overall performance.

Investment analysts are required to follow the rules established by the National Association of Securities Dealers (NASD), which is the world's leading private-sector provider of financial regulatory services.

Some examples of the NASD's rules are listed next.

- Research analysts employed by NASD members must register with the NASD and must pass a qualification examination and comply with a continuing education requirement.
- Broker-dealers must disclose the percentage breakdown of their buy, hold, and sell recommendations.
- The firm cannot retaliate against analysts for unfavorable or negative research or ratings.
- Securities analysts are freed from the supervision and control of investment banking management regarding compensation, pending research reports, and the extent of coverage of a company.
- Broker-dealer firms and their analysts must disclose ownership of common shares in the securities of a recommended issuer.
- Each participating investment bank must hire at least three independent securities analysts.

(e) Handling Employees

Handling employees and unions is a sensitive matter because people are the most valuable asset of an organization. Management needs to be familiar with applicable laws and regulations in this matter.

According to Business Roundtable, these guidelines apply when developing relationships with employees:

- It is in a corporation's best interest to treat employees fairly and equitably.
- Corporations should have in place policies and practices that provide employees with compensation, including benefits, that are appropriate given the nature of the corporation's business and employees' job responsibilities and geographic locations.
- When corporations offer retirement, health care, insurance, and other benefit plans, employees should be fully informed of the terms of those plans.
- Corporations should have in place and publicize mechanisms for employees to seek guidance and to alert management and the board about potential or actual misconduct without fear of retribution.
- Corporations should communicate honestly with their employees about corporate operations and financial performance.[11]

Companies are encouraged, and in some countries even obliged, to provide information on key issues relevant to employees and other stakeholders that may materially affect the performance of the company. Disclosure may include management and employee relations and relations with other stakeholders, such as unions.

Some countries require extensive disclosure of information on human resources (HR). HR policies, such as programs for HR development and training, retention rates of employees, and employee share ownership plans, can communicate important information on the competitive strengths of companies to market participants.

(i) Prohibited Personnel Practices with Employees

In a high-performing workplace, employees must be able to pursue the missions of their organizations free from discrimination and should not fear or experience retaliation or reprisal for reporting—blowing the whistle on—waste, fraud, and abuse. Laws should protect employees from discrimination based on their race, color, sex, religion, national origin, age, or disability, as well as from retaliation for filing a complaint of discrimination. For example, U.S. federal employees are protected from these 12 prohibited personnel practices:[12]

1. Unlawful discrimination
2. Solicitation or consideration of improper background references
3. Coercion of political activity
4. Obstruction of the right to compete

[11] Ibid.

[12] General Accounting Office, "Whistleblower Protection: VA Did Little Until Recently to Inform Employees About Their Rights" (GAO/GGD-00-70), April 2000. www.gao.gov/assets/240/230214.pdf

5. Influencing withdrawal of applicants from competition
6. Unauthorized references
7. Nepotism
8. Reprisal for whistleblowing
9. Reprisal for the exercise of an appeal right
10. Discrimination based on off-duty conduct
11. Violation of laws or regulations implementing or concerning merit system principles
12. Violation of veterans' preference

(ii) Protecting Whistleblowing Employees

Whistleblower reprisal is generally defined as employers' taking or threatening to take personnel action against employees for reporting a violation of law, rule, or regulation; or gross mismanagement; gross waste of funds, abuse of authority, or a substantial and specific danger to public health or safety. Under the U.S. Whistleblower Protection Act of 1994 and the Notification and Federal Employee Anti-discrimination and Retaliation Act of 2001 (No FEAR Act), federal agencies are responsible for the prevention of reprisal to their employees.[13]

Private sector organizations, like public sector organizations, should develop policies and procedures to protect whistleblowing employees and to prevent the reprisal to their employees.

Possible negative actions of management if employees report misconduct:

- Deny expected cash award or bonus
- Deny expected promotion
- Dismissal
- Duties or responsibilities reduced or lowered
- Harassment
- Lower next performance appraisal
- Reassignment of work location
- Social isolation by peers
- Reassignment of work schedule

Possible positive actions by management if employees report misconduct:

- Positive recognition by management
- Positive support by peers
- Promotion
- Employee self-satisfaction

[13] Ibid.

(f) Dealing with Labor Unions

Employees who belong to collective bargaining units represented by labor unions can also file grievances over discrimination and reprisal allegations under the terms of collective bargaining agreements. In those situations, the employee must choose to seek relief either under the statutory procedure or under the negotiated grievance procedure, but not both. U.S. employers must comply with the Wagner Act of 1935, which prohibits employers from undertaking unfair labor practices. For example, employers should not stop employees joining labor unions.

A brief overview of labor unions in selected countries is presented next.

- Labor union members as a percentage of the total workforce slowly declined in the United States.
- Due to a cultural emphasis on harmony and nonconfrontation, labor unions are discouraged in Japan.
- Labor unions in Ireland are not as strong as they are in France and Germany.
- Labor unions in Germany, although slowly declining in numbers, exercise a great deal of power over management decisions in establishing company strategies and policies by participating in management meetings and by exercising voting power on management's proposed actions.
- Due to global mobility of workers, labor unions in different countries are competing against one another, thus creating a downward pressure on both wages and union power worldwide.

(g) Handling Regulators and Government Authorities

If new laws and regulations are needed, such as to deal with clear cases of market imperfections, they should be designed in a way that makes them possible to implement and enforce in an efficient and evenhanded manner covering all parties. Consultation by government and other regulatory authorities with corporations, their representative organizations, and other stakeholders is an effective way of doing this. Mechanisms should also be established for parties to protect their rights. In order to avoid overregulation, unenforceable laws, and unintended consequences that may impede or distort business dynamics, policy measures should be designed with a view to their overall costs and benefits. Such assessments should take into account the need for effective enforcement, including the ability of authorities to deter dishonest behavior and to impose effective sanctions for violations.

According to Business Roundtable, these guidelines apply when developing relationships with government.[14]

- Corporations, like all citizens, must act within the law. The penalties for serious violations of law can be extremely severe, even life threatening, for corporations. Compliance is not only appropriate; it is essential. Management should take reasonable steps to develop, implement, and maintain an effective legal compliance program, and the board should be knowledgeable about and oversee the program, including periodically reviewing the program to gain reasonable assurance that it is effective in deterring and preventing misconduct.

[14] *Principles of Corporate Governance*, p. 34.

- Corporations have an important perspective to contribute to the public policy dialogue and should be actively involved in discussions about the development, enactment, and revision of the laws and regulations that affect the businesses and the communities in which they operate and their employees reside.

(i) Securities and Exchange Commission

Of all the regulators and government authorities, business corporations deal with the Securities and Exchange Commission (SEC) staff more often due to federal securities laws such as the Securities Act of 1933, the Securities Exchange Act of 1934 (the Exchange Act), and the Sarbanes-Oxley Act of 2002 (SOX).

Federal securities laws help to protect the investing public by requiring public companies to disclose financial and other information. SEC was established by the Exchange Act to operationalize and enforce securities laws and to oversee the integrity and stability of the market for publicly traded securities. SEC is the primary U.S. federal agency involved in accounting requirements for publicly traded companies. Under Section 108 of SOX, SEC has recognized the accounting standards set by the Financial Accounting Standards Board (FASB)—generally accepted accounting principles (GAAP)—as "generally accepted" for the purpose of the federal securities laws. SEC reviews and comments on registrant filings and issues interpretive guidance and staff accounting bulletins on accounting matters.

(ii) SEC Enforcement Process

The SEC investigates possible violations of securities laws, including those related to accounting issues. If the evidence gathered merits further inquiry, the SEC will prompt an informal investigation or issue a formal order of investigation. Investigations can lead to SEC-prompted administrative or federal civil court actions. Depending on the type of proceedings, the SEC can seek sanctions that include injunctions, civil money penalties, disgorgement (i.e., return of illegal profits), cease-and-desist orders, suspensions of registration, bars from appearing before the SEC, and officer and director bars. After an investigation is completed, the SEC may institute either type of proceeding against a person or entity that it believes has violated federal securities laws. The SEC can also initiate contempt proceedings and issue reports of investigation when appropriate. Because the SEC has only civil enforcement authority, it may also refer appropriate cases to the U.S. Department of Justice for criminal investigation and prosecution. According to the SEC, most enforcement actions are settled, with respondents generally consenting to the entry of civil judicial or administrative orders without admitting or denying the allegations against them.

(h) Handling Suppliers, Vendors, Contractors, and Customers

Companies are encouraged, and in some countries even obliged, to provide information on key issues relevant to stakeholders that may materially affect the performance of the company. Disclosure may include relations with stakeholders such as creditors, suppliers, and local communities. Because suppliers, vendors, contractors, and customers are organization outsiders, they can provide feedback, outside-in perspectives, and candid opinions about company products, services, or standard operating procedures and their deficiencies the way they see them. Organizations should view this feedback seriously and correct the deficiencies with due care and due diligence.

(i) Dealing with Suppliers, Vendors, and Contractors

Most suppliers, vendors, and contractors are ethical and honest; however, there are a few that are not. Organizations must be vigilant regarding the possibility of vendor fraud as it can occur in several forms, such as overcharging for purchased goods, shipping inferior-quality goods, or not shipping goods even though payment was made. Also, there is a possibility of collusion among buyers and vendors, suppliers, and contractors.

Organizations should note these issues about their suppliers, vendors, and contractors:

- A vendor can provide information regarding completed or open shipments, which can be used in identifying and correcting discrepancies and reconciling account balances. The same thing may hold true with billings or invoices.
- A supplier can become a whistleblower and notify company management of a purchasing agent or buyer's request for a kickback or bribe.
- A contractor, who is a previous employee of a company, may pose tax and legal problems.

When dealing with suppliers, vendors, and contractors, organizations should:

- Develop a single, broad, goal-based supplier management policy.
- Balance between risks and rewards.
- Promote competition in managing multiple tiers of the supplier base, knowing that competition drives quality and innovation.
- Establish an accountability chain in the purchasing organization so that a manager's actions are linked to performance. Apply the same chain throughout the management hierarchy.
- Provide for timely oversight role over the outsource vendor.
- Develop a flexible acquisition strategy for innovative products and services.
- Use vendor's past performance as the primary selection criterion to help ensure that poor-performing suppliers are not reemployed simply by underbidding other suppliers.
- Establish metrics that assess capabilities delivered and management of cost, schedule, and performance issues (e.g., earned value management technique).
- Use competitive sourcing and best practices to increase innovation, efficiency, and effectiveness.

Organizations should not use cost as a primary driver for selecting suppliers, vendors, and contractors; instead, they should use quality, performance, and standards.

(ii) Dealing with Customers

Most customers are ethical and honest; however, there are a few that are not. Organizations must be vigilant of customer fraud, such as not paying for goods shipped with the hope of getting something for nothing or creating unnecessary disputes over billing with the hope that the company would eventually forgive and forget about the billing.

Some customers may inform a company about shipping delays, billing problems, inferior product quality, and poor service quality, or may express their overall dissatisfaction with products or

services. These are examples of the reactive style. Companies should respect customers and pay attention to their complaints and suggestions (i.e., outside-in perspective).

Proactive customers may work with an organization in developing new product or service requirements and/or product or service enhancements (i.e., voice of the customer or house of quality). This proactive style reflects doing things right at the first time, which will help both the customer and the organization.

Customer surveys can help organizations in receiving problem-related information at the right time to investigate the underlying source of the problem and correct it.

(i) Dealing with Purchasing Agents, Buyers, or Commodity/Service Experts

Corporate management can reduce unethical or illegal behavior of purchasing agents, buyers, or commodity/service experts, and salespeople with a policy and code of conduct statement combined with appropriate punishment to those who conduct themselves improperly.

Purchasing managers, more than any other management group within an organization, face enormous pressure to act in unethical way. This occurs for several reasons. First, purchasing has direct control over large sums of money. A buyer responsible for a multimillion-dollar contract may find sellers using any means available to secure a favorable position. The very nature of purchasing means that a buyer must come in contact with outside, and occasionally, unethical sellers. A second reason is due to the pressure placed on many salespeople. A seller who must meet aggressive sales goals might resort to questionable sales practices, which, in turn, influence buying practices.

Three rules must be understood as part of purchasing buyer behavior.

1. A buyer must commit attention and energies for the organization's benefit rather than for personal enrichment at the expense of the organization. Ethical buyers do not accept outside gifts or favors that violate their company's ethical policy. Ethical buyers are also not tempted or influenced by the unethical practices of salespeople and do not have personal financial arrangements with suppliers.
2. A buyer must act ethically toward suppliers or potential suppliers. This means treating each supplier professionally and with respect.
3. A buyer must uphold the ethical standards set forth by his or her profession. A code of professional ethics usually formalizes the set of ethical standards.

Organizations must take the next steps to enhance the ethical behavior of their purchasing personnel.

- Install buying teams to evaluate potential suppliers across different performance categories or selection criteria. Using a team approach to evaluate a supplier's capabilities limits the opportunity for unethical behavior.
- Develop a formal ethics policy defining the boundaries of ethical behavior, such as accepting gifts and receiving other favors.
- Communicate top management's message to buyers about whether unethical behavior is tolerated.

- Develop systems for internal reporting of unethical behavior, such as a fraud hotline.
- Rotate buyers among different purchasing items or commodities to prevent a buyer from becoming too comfortable with any particular group of suppliers. This is to prevent collusion between buyers and vendors, suppliers, and contractors.
- Develop a policy to limit a buyer's authority for awarding purchase contracts, say, to amounts of $10,000 or less. Contracts greater than $10,000 requires a manager's signature, and the signature chain continues up the management hierarchy with the increased purchase contract amounts.
- Provide ethical training.

(j) Dealing with Marketing and Salespeople

A policy should be established prohibiting marketing and salespeople to distribute gifts and favors in the process of acquiring new customers and retaining current customers. This policy should be consistent with the policy prohibiting purchasing personnel from accepting gifts and favors from new suppliers as well as current suppliers. Other illegal and unethical practices that should be prohibited include price discrimination, misleading advertising, defrauding customers with false claims, unfair credit practices, price collusion with competing firms, and sexual harassment. This policy should be referred to and linked to the company's code of conduct statement.

(k) Handling Related Parties and Third Parties

It is important for the market to know whether the company is being run with due regard to the interests of all its investors. To this end, it is essential for the company to fully disclose material related-party transactions to the market, either individually or in a grouped basis, including whether they have been executed at arm's length and on normal market terms. In a number of jurisdictions, this is indeed already a legal requirement. Related parties can include entities that control or are under common control of the company, significant shareholders including members of their families, and key management personnel.

Examples of Related Party Transactions

- Misreported sales between affiliates
- Unspecified intercompany transactions
- Failure to disclose and account for a compensation arrangement with a former chief executive
- Personal loans to the current chief executive or other executives

Transactions involving the major shareholders (e.g., close family and relations), either directly or indirectly, are potentially the most difficult type to deal with. In some jurisdictions, shareholders above a limit as low as 5% shareholdings are obliged to report transactions. Disclosure requirements include the nature of the relationship where control exists and the nature and amount of transactions with related parties, grouped appropriately. Given the inherent opaqueness of many transactions, the beneficiary may be obliged to inform the board about the transaction, which in turn should make a disclosure to the market. This should not absolve the company from maintaining its own monitoring, which is an important task for the board.

(l) Handling Business Mergers, Acquisitions, and Divestitures

In some countries, companies employ anti-takeover devices or tactics during business mergers and acquisitions. However, both investors and stock exchanges have expressed concern over the possibility that widespread use of anti-takeover devices may be a serious impediment to the functioning of the market for corporate control. In some instances, takeover defenses can simply be devices to shield the management or the board from shareholder monitoring. In implementing any anti-takeover devices and in dealing with takeover proposals, the fiduciary duty of the board to shareholders and the company must remain paramount.

4.3 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Which of the following enables communicators to know if their message has been understood?

a. Encoding

b. Decoding

c. Feedback

d. Perception

2. Which of the following refers to the unofficial and informal communication system in an organization?

a. Grapevine

b. Water fountain talks

c. Hallway gossiping

d. Cafeteria chatting

3. Most managers have which one of the following attitudes toward the grapevine?

a. Positive

b. Uncertain

c. Negative

d. Neutral

4. Communication channel richness refers to which of the following?

a. Number of messages a channel can carry at one time

b. Speed in which messages can be carried

c. Amount of information that can be transmitted during a communication episode

d. Number of channels available at any one time

5. Which of the following is the **richest** medium for communication?

a. Telephone conversations

b. Face-to-face discussions

c. Electronic media

d. Written media

6. When dealing with employees, which of the following is **not** an example of possible management's negative actions if whistleblowing employees report misconduct of management?

a. Reduced duties

b. Coercion of political activity

c. Reassignment of work location

d. Reshuffling of work schedules

7. Which of the following was **not** a major shareholder initiative?

a. Rise of shareholder activist groups

b. Shareholder-initiated golden parachutes

c. Shareholder resolutions and annual meetings

d. Shareholder lawsuits

8. When dealing with stakeholders, which of the following ethical and legal principles is **not** applicable?

a. Due process

b. Due diligence

c. Due care

d. Duty of loyalty

9. Which of the following is the **ultimate** goal of shareholder and investor communications?

a. Honesty

b. Consistency

c. Clarity

d. Effectiveness

10. When handling related parties, which of the following is the **most** difficult type of transaction?

a. Misreported sales between affiliates

b. Unspecified intercompany transactions

c. Personal loans to the current chief executive

d. A close family who is a major shareholder

DOMAIN 5

Management and Leadership Principles (10–20%)

5.1 Strategic Management

Topics such as the strategic management process, forecasting, quality management, and decision analysis, including the problem-solving framework, are discussed in this section.

(a) Strategic Management Defined

(i) Strategic Management Process

Strategic management is the set of decisions and actions used to formulate and implement strategies that will provide a competitively superior fit between the organization and its environment so as to achieve organizational goals. Managers ask questions such as: What changes and trends are occurring in the competitive environment? Who are our customers? What products or services should we offer? How can we offer those products and services most efficiently? Answers to these questions help managers make choices about how to position their organization in the environment with respect to rival companies. Superior organizational performance is not a matter of luck. It is determined by the choices that managers make. Top executives use strategic management to define an overall direction for the organization, which is the firm's grand strategy. The strategic management process is defined as a series of these activities:

Grand Strategy → Strategy Formulation (Planning) → Strategy Implementation → Strategic Control

(ii) Grand Strategy

The grand strategy is the general plan of major action by which a firm intends to achieve its long-term goals. Grand strategies can be defined for four general categories: (1) growth, (2) stability, (3) retrenchment, and (4) global operations.

Growth can be promoted internally by investing in expansion or externally by acquiring additional business divisions. Internal growth can include development of new or changed products or expansion of current products into new markets. External growth typically involves *diversification*, which means the acquisition of businesses that are related to current product lines or that take the corporation into new areas. The number of companies choosing to grow through mergers and acquisitions (M&A) is astounding, as organizations strive to acquire the size and resources to compete on a global scale, to invest in new technology, and to control distribution channels and guarantee access to markets.

Stability, sometimes called a *pause strategy*, means that the organization wants to remain the same size or grow slowly and in a controlled fashion. The corporation wants to stay in its current business. After organizations have undergone a turbulent period of rapid growth, executives often focus on a stability strategy to integrate strategic business units and to ensure that the organization is working efficiently.

Retrenchment means that the organization goes through a period of forced decline by either shrinking current business units or selling off or liquidating entire businesses. The organization may have experienced a precipitous drop in demand for its products or services, prompting managers to order across-the-board cuts in personnel and expenditures. **Liquidation** means selling off a business unit for the cash value of the assets, thus terminating its existence. **Divestiture** involves the selling off of businesses that no longer seem central to the corporation. Studies show that between 33% and 50% of all acquisitions are later divested. Retrenchment is also called downsizing.

In today's **global operations**, senior executives try to formulate coherent strategies to provide synergy among worldwide operations for the purpose of fulfilling common goals. Each country or region represents a new market with the promise of increased sales and profits. In the international arena, companies face a strategic dilemma between global integration and national responsiveness. Organizations must decide whether they want each global affiliate to act autonomously or whether activities should be standardized and centralized across countries. This choice leads managers to select a basic grand strategy alternative, such as globalization versus multidomestic strategy. Some corporations may seek to achieve both global integration and national responsiveness by using a transnational strategy.

When an organization chooses a strategy of **globalization**, its product design and advertising strategies are standardized throughout the world. This approach is based on the assumption that a single global market exists for many consumer and industrial products. The theory is that people everywhere want to buy the same products and live the same way. A globalization strategy can help an organization reap efficiencies by standardizing product design and manufacturing, using common suppliers, introducing products around the world faster, coordinating prices, and eliminating overlapping facilities. Globalization enables marketing departments alone to save millions of dollars.

When an organization chooses a **multidomestic strategy,** competition in each country is handled independently of industry competition in other countries. Thus, a multinational company is present in many countries, but it encourages marketing, advertising, and product design to be modified and adapted to the specific needs of each country. Many companies reject the idea of a single global market.

A **transnational strategy** seeks to achieve both global integration and national responsiveness. A true transnational strategy is difficult to achieve because one goal requires close global coordination while the other goal requires local flexibility. However, many industries are finding that, although increased competition means they must achieve global efficiency, growing pressure to meet local needs demands national responsiveness.

Although most multinational companies want to achieve some degree of global integration to hold costs down, even global products may require some customization to meet government regulations in various countries or some tailoring to fit consumer preferences. In addition, some products are better suited for standardization than others. Most large multinational corporations with diverse products will attempt to use a partial multidomestic strategy for some product lines and global strategies for others. Coordinating global integration with responsiveness to the heterogeneity of international markets is a difficult balancing act for managers, but it is an increasingly important one in today's global business world.

KEY CONCEPTS TO REMEMBER: Vocabulary Related to Strategic Management

- **Organizational goal.** An organizational goal is a desired state of affairs that the organization attempts to reach. A goal represents a result or an end point toward which organizational efforts are directed. The choice of goals and strategy affects organization design. Top managers give direction to organizations. They set goals and develop the strategies for their organization to attain those goals.
- **Organizational purpose.** Organizations are created and continued in order to accomplish something. This purpose may be referred to as the overall goal, or mission. Different parts of the organization establish their own goals and objectives to help meet the overall goal, mission, or purpose of the organization.

  Many types of goals exist in an organization, and each type performs a different function. One major distinction is between the officially stated goals, or mission, of the organization and the operative goals that the organization actually pursues.
- **Mission.** The overall goal for an organization is often called the mission—the organization's reason for existence. The mission describes the organization's vision, its shared values and beliefs, and its reason for being. It can have a powerful impact on an organization. The mission is sometimes called the official goals, which are the formally stated definition of business scope and outcomes the organization is trying to achieve. Official goal statements typically define business operations and may focus on values, markets, and customers that distinguish the organization. Whether called a mission statement or official goals, the organization's general statement of its purpose and philosophy is often written down in a policy manual or the annual report.
- **Operative goals.** Operative goals designate the ends sought through the actual operating procedures of the organization and explain what the organization is actually trying to do. Operative goals describe specific measurable outcomes and are often concerned with the short run. Operative versus official goals represent actual versus stated goals. Operative goals typically pertain to the primary tasks an organization must perform, similar to the subsystem activities. These goals concern overall performance, boundary spanning, maintenance, adaptation, and production activities. Specific goals for each primary task provide direction for the day-to-day decisions and activities within departments.

- **Purpose of strategy.** A strategy is a plan for interacting with the competitive environment to achieve organizational goals. Some managers think of goals and strategies as interchangeable, but for our purposes, goals define where the organization wants to go and strategies define how it will get there. For example, a goal may be to achieve 15% annual sales growth; strategies to reach that goal might include aggressive advertising to attract new customers, motivating salespeople to increase the average size of customer purchases, and acquiring other businesses that produce similar products.

  Strategies can include any number of techniques to achieve the goal. The essence of formulating strategies is choosing whether the organization will perform different activities from its competitors or will execute similar activities more efficiently than its competitors do.

  Within the overall grand strategy of an organization, executives define an explicit strategy, which is the plan of action that describes resource allocation and activities for dealing with the environment and attaining the organization's goals. The essence of formulating strategy is choosing how the organization will be different. Managers make decisions about whether the company will perform different activities or will execute similar activities differently than its competitors do. Strategy necessarily changes over time to fit environmental conditions, but to remain competitive, companies develop strategies that focus on core competencies, develop synergy, and create value for customers.

  A company's core competence is something the organization does especially well in comparison to its competitors. A core competence represents a competitive advantage because the company acquires expertise that competitors do not have. A core competence may be in the area of superior research and development (R&D), expert technological know-how, process efficiency, or exceptional customer service.

  When organizational parts interact to produce a joint effect that is greater than the sum of the parts acting alone, synergy occurs. The organization may attain a special advantage with respect to cost, market power, technology, or management skill. When properly managed, synergy can create additional value with existing resources, providing a big boost to the bottom line. Synergy can also be obtained through good relations with suppliers or by strong alliances among companies.

  Delivering value to the customer should be at the heart of strategy. Value can be defined as the combination of benefits received and costs paid by the customer. Managers help their companies create value by devising strategies that exploit core competencies and attain synergy.

- **Levels of strategy.** Another aspect of strategic management concerns the organizational level to which strategic issues apply. Strategic managers normally think in terms of three levels of strategy: corporate, business, and functional.

  The question "What business are we in?" concerns corporate-level strategy. Corporate-level strategy pertains to the organization as a whole and the combination of business units and product lines that make up the corporate entity. Strategic actions at this level usually relate to the acquisition of new businesses; additions or divestments of business units, plants, or product lines; and joint ventures with other corporations in new areas.

  The question "How do we compete?" concerns business-level strategy. Business-level strategy pertains to each business unit or product line. It focuses on how the business unit competes within its industry for customers. Strategic decisions at the business level concern amount of advertising, direction and extent of R&D, product changes, new-product development, equipment and facilities, and expansion or contraction of product lines. Many companies are opening e-commerce units as a part of business-level strategy.

  The question "How do we support the business-level competitive strategy?" concerns functional-level strategy. It pertains to the major functional departments within the business unit. Functional strategies involve all of the major functions, including finance, R&D, marketing, and manufacturing.

- **Partnership strategies and business ecosystems.** So far, we have been discussing strategies that are based on how to compete with other companies. An alternative approach to strategy emphasizes collaboration. In some situations, companies can achieve competitive advantages by cooperating with other firms rather than competing. Partnership strategies are becoming increasingly popular as firms in all industries join with other organizations to promote innovation, expand markets, and pursue joint goals. Partnering was once a strategy adopted primarily by small firms that needed greater marketing muscle or international access. Today, however, it has become a way of life for most companies, large and small. The question is no longer whether to collaborate but rather where, how much, and with whom to collaborate. Competition and cooperation often exist at the same time representing business ecosystems. The Internet is both driving and supporting the move toward partnership thinking.

  Mutual dependencies and partnerships have become a fact of life, but the degree of collaboration varies. Organizations can choose to build cooperative relationships in many ways, such as through preferred suppliers, strategic business partnering, joint ventures, or M&A. A still higher degree of collaboration is reflected in joint ventures, which are separate entities created with two or more active firms as sponsors. M&A represent the ultimate step in collaborative relationships. U.S. business has been in the midst of a tremendous M&A boom.

  Today's companies embrace both competition and cooperation simultaneously. Few companies can go it alone under a constant onslaught of international competition, changing technology, and new regulations. In this new environment, businesses choose a combination of competitive and partnership strategies that add to their overall sustainable advantage.

  Overall effectiveness is difficult to measure in organizations. Organizations are large, diverse, and fragmented. They perform many activities simultaneously and pursue multiple goals. They also generate many outcomes, some intended and some unintended. Managers determine which indicators to measure in order to gauge the effectiveness of their organizations. One study found that many managers have a difficult time with the concept of evaluating effectiveness based on characteristics that are not subject to hard, quantitative measurement. However, top executives at some of today's leading companies are finding new ways to measure effectiveness, using indicators such as "customer delight" and employee satisfaction. A number of approaches to measuring effectiveness look at which measurements the organization managers choose to track. These contingency effectiveness approaches are based on looking at which part of the organization managers consider most important to measure.

- **Contingency effectiveness approaches.** Contingency approaches to measuring effectiveness focus on different parts of the organization. Traditional approaches include the goal approach, the resource-based approach, and the internal process approach. Organizations bring resources in from the environment, and those resources are transformed into outputs delivered back into the environment. The goal approach to organizational effectiveness is concerned with the output side and whether the organization achieves its goals in terms of desired levels of output. The resource-based approach assesses effectiveness by observing the beginning of the process and evaluating whether the organization effectively obtains resources necessary for high performance. The internal process approach looks at internal activities and assesses effectiveness by indicators of internal health and efficiency.

  These traditional approaches all have something to offer, but each one tells only part of the story. A more recent stakeholder approach (also called the constituency approach) acknowledges that each organization has many constituencies that have a stake in its outcomes. The stakeholder approach focuses on the satisfaction of stakeholders as an indicator of the organization's performance.

(iii) Strategy Formulation (Planning)

The overall strategic management process begins when executives evaluate their current position with respect to mission, goals, and strategies. They then scan the organization's internal and external environments and identify strategic factors that might require change. Internal or external events might indicate a need to redefine the mission or goals or to formulate (plan) a new strategy at the corporate, business, or functional level. The next stage is implementation of the new strategy. The final stage is strategic control to keep strategic plans on track.

Strategy formulation includes the planning and decision making that lead to the establishment of the firm's goals and the development of a specific strategic plan. Strategy formulation may include assessing the external environment and internal problems and integrating the results into goals and strategy. This is in contrast to strategy implementation, which is the use of managerial and organizational tools to direct resources toward accomplishing strategic results. Strategy implementation is the administration and execution of the strategic plan. Managers may use persuasion, new equipment, changes in organization structure, or a reward system to ensure that employees and resources are used to make formulated strategy a reality.

WHAT IS STRATEGIC MANAGEMENT?

Strategic management is strategic formulation (planning) plus strategic implementation plus strategic control.

Formulating (planning) strategy often begins with an assessment of the internal and external factors that will affect the organization's competitive situation. Situation analysis typically includes a search for SWOT (strengths, weaknesses, opportunities, and threats) that affect organizational performance. Situation analysis is important to all companies but is crucial to those considering globalization because of the diverse environments in which they will operate. External information about opportunities and threats may be obtained from a variety of sources, including customers, government reports, professional journals, suppliers, bankers, friends in other organizations, consultants, and association meetings. Many firms hire special scanning organizations to provide them with newspaper clippings, Internet research, and analyses of relevant domestic and global trends. Some firms use more subtle techniques to learn about competitors, such as asking potential recruits about their visits to other companies, hiring people away from competitors, debriefing former employees or customers of competitors, taking plant tours posing as "innocent" visitors, and even buying competitors' garbage. In addition, many companies are hiring competitive intelligence professionals to scope out competitors.

Executives acquire information about internal strengths and weaknesses from a variety of reports, including budgets, financial ratios, profit and loss statements, and surveys of employee attitudes and satisfaction. Managers spend 80% of their time giving and receiving information. Through frequent face-to-face discussions and meetings with people at all levels of the hierarchy, executives build an understanding of the company's internal strengths and weaknesses.

Internal strengths are positive internal characteristics that the organization can exploit to achieve its strategic performance goals. **Internal weaknesses** are internal characteristics that might inhibit or restrict the organization's performance. The information sought typically pertains to specific functions, such as marketing, finance, production, and R&D. Internal analysis also examines overall organization structure, management competence and quality, and human

resource (HR) characteristics. Based on their understanding of these areas, managers can determine their strengths or weaknesses vis-à-vis other companies.

External threats are characteristics of the external environment that may prevent the organization from achieving its strategic goals. **External opportunities** are characteristics of the external environment that have the potential to help the organization achieve or exceed its strategic goals. Executives evaluate the external environment with information about nine sectors. The task environment sectors are the most relevant to strategic behavior and include the behavior of competitors, customers, suppliers, and the labor supply. The general environment contains those sectors that have an indirect influence on the organization but nevertheless must be understood and incorporated into strategic behavior. The general environment includes technological developments, the economy, legal-political and international events, and sociocultural changes. Additional areas that might reveal opportunities or threats include pressure groups, interest groups, creditors, natural resources, and potentially competitive industries.

(iv) Strategy Implementation

The next step in the strategic management process is **implementation**—how strategy is put into action. Some people argue that strategy implementation is the most difficult and important part of strategic management. No matter how creative the formulated strategy, the organization will not benefit if the strategy is incorrectly implemented. In today's competitive environment, there is an increasing recognition of the need for more dynamic approaches to formulating as well as implementing strategies. Strategy is not a static, analytical process; it requires vision, intuition, and employee participation. Many organizations are abandoning central planning departments, and strategy is becoming an everyday part of the job for workers at all levels. Strategy implementation involves using several tools—parts of the firm that can be adjusted to put strategy into action. Once a new strategy is selected, it is implemented through changes in leadership, structure, information and control systems, and employee. For strategy to be implemented successfully, all aspects of the organization need to be in concert with the strategy. Implementation involves regularly making difficult decisions about doing things in a way that supports rather than undermines the organization's chosen strategy.

The difficulty of implementing strategy is greater when a company goes global. In the international arena, flexibility and superb communication emerge as mandatory leadership skills. Likewise, structural design must merge successfully with foreign cultures as well as link foreign operations to the home country. Managers must make decisions about how to structure the organization to achieve the desired level of global integration and local responsiveness. Information and control systems must fit the needs and incentives within local cultures. In a country such as Japan or China, financial bonuses for star performance would be humiliating to an individual whereas group motivation and reward are acceptable. As in North America, control typically is created through timetables and budgets and by monitoring progress toward desired goals. Finally, the recruitment, training, transfer, promotion, and layoff of international employees create an array of problems not confronted in North America. Labor laws, guaranteed jobs, and cultural traditions of keeping unproductive employees on the job provide special problems for strategy implementation.

In summary, strategy implementation is essential for effective strategic management. Managers implement strategy through the tools of leadership, structural design, information and control systems, and employees. Without effective implementation, even the most creative strategy will fail.

(v) Strategic Control

A formal control system can help keep strategic plans on track. A control system (e.g., reward systems, pay incentives, budgets, information technology (IT) systems, rules, policies, and procedures) should be proactive instead of reactive. Control should not stifle creativity and innovation since there is no trade-off between control and creativity. Feedback is part of control.

The goal of a control system is to detect and correct problems in order to keep plans on target. This means negative results should prompt corrective action at the steps immediately before and after the problem identification. Some examples of corrective actions include updating assumptions, reformulating plans, rewriting policies and procedures, making personnel changes, modifying budget allocations, and improving IT systems.

(b) Strategic Planning Process

The output of the strategic planning process is the development of a strategic plan. Its four components include: (1) mission, (2) objectives, (3) strategies, and (4) portfolio plan (see Exhibit 5.1).

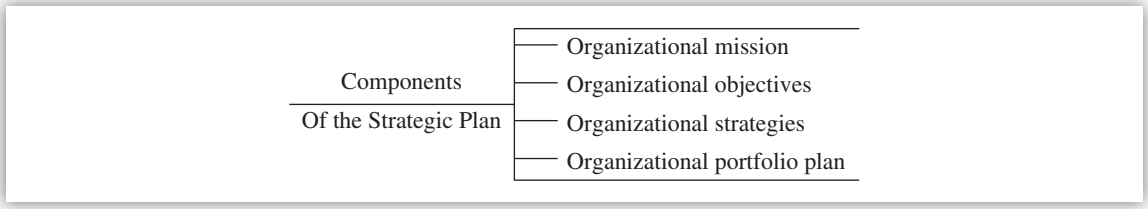


EXHIBIT 5.1 Components of the Strategic Planning Process

(i) Organizational Mission

Every organization exists to accomplish something, and the mission statement is a reflection of this. The mission statement of an organization should be a long-term vision of what the organization is trying to become, the unique aim that differentiates the organization from similar ones. The mission statement raises questions such as: What is our business? and What should it be? In developing a statement of mission, management must take into account three key elements: the organization's history, its distinctive competencies, and its environment.

The organization's environment dictates the opportunities, constraints, and threats that must be identified before a mission statement is developed.

When completed, an effective mission statement focuses on markets rather than products and is achievable, motivating, and specific. A key feature of mission statements has been an external rather than an internal focus. This means that a mission statement should focus on the broad class of needs that the organization is seeking to satisfy (external focus), not on the physical product or service that the organization is offering at present (internal focus). As Peter Drucker puts it, the question "What is our business?" can be answered only by looking at the business from the outside, from the point of view of customer and market.

WHAT IS OUR BUSINESS?

- A business is defined by the want the customer satisfies when he or she buys a product or service.
- Satisfying the customer is the mission and purpose of every business.

A mission statement should be realistic and achievable and should not lead the organization into unrealistic ventures far beyond its competencies. A mission statement is a guide to all employees and provides a shared sense of purpose that offers a strong motivation to achieve objectives of the organization.

A mission statement must be specific to provide direction to management when it is choosing between alternative courses of action. For example, a mission to provide the highest-quality products at the lowest possible cost sounds good, but it is not specific enough to be useful. Specific quantitative goals are easier to measure.

(ii) Organizational Objectives

An organization's mission is converted into specific, measurable, and action-oriented commitments and objectives. These objectives, in turn, provide direction, establish priorities, and facilitate management control. When these objectives are accomplished the organization's mission is also accomplished. Peter Drucker advises at least eight areas for establishing objectives, including:

1. Market standing
2. Innovations
3. Productivity
4. Physical and financial resources
5. Profitability
6. Manager performance and responsibility
7. Worker performance and attitude
8. Social responsibility

(iii) Organizational Strategies

Organizational strategy involves identifying the general approaches a business should take in order to achieve its objectives. It sets the major directions for the organization to follow. Specific steps include understanding and managing the current customer and current products and identifying new customers and new products. *Mission and objectives lead an organization where it wants to go. Strategies help an organization to get there.*

Marketing writers describe organizational strategy in terms of a product/market matrix. The matrix is shown in Exhibit 5.2.

	Current products	**New products**
Current customers	Market penetration	Product development
New customers	Market development	Diversification

EXHIBIT 5.2 Product/Market Matrix

Market penetration strategy focuses on improving the position of the present product with its current customers. It involves designing a marketing plan to encourage customers to purchase more of a product. It can also include a production plan to produce more efficiently than what is being produced at present. **Market development strategy** would seek to find new customers for current products. With the **product development strategy,** new

products are developed to direct to current customers. **Diversification strategy** seeks new products for new customers.

(iv) Organizational Portfolio Plan

An organization can be thought of as a portfolio of businesses (i.e., combination of product lines and divisions, and service lines and divisions). It is understandable that some product lines will be more profitable than others. Management must decide which product lines or divisions to build, maintain, add, and eliminate.

(c) Global Analytical Techniques

Global analytical techniques include structural analysis of industries, competitive strategies, competitive analysis, market signals, and industry evolution. This section is adapted from Michael E. Porter's book titled *Competitive Strategy.*[1]

(i) Structural Analysis of Industries

The essence of formulating competitive strategy is relating a company to its environment—that is, the industry or industries in which it operates and competes. Structural analysis is the fundamental base for formulating competitive strategy. Porter's five competitive forces are at work on an industry, including:

1. Threat of new entrants
2. Rivalry among existing firms
3. Pressure from substitute products or services
4. Bargaining power of buyers
5. Bargaining power of suppliers

All five competitive forces jointly determine the intensity of industry competition and profitability.

(A) Threat of New Entrants New entrants to an industry bring new capacity and the desire to gain market share. They often also bring substantial resources. As a result, prices can be low, costs can be high, and profits can be low. There is a relationship among threat of new entrants, barriers to entry, and reaction from existing competitors. For example:

- If barriers are high and reaction is high, then the threat of entry is low.
- If barriers are low and reaction is low, then the threat of entry is high.

There are seven major barriers to entry:

1. Economies of scale
2. Product differentiation
3. Capital requirements

[1] Michael E. Porter, *Competitive Strategy* (New York: Free Press, 1980).

4. Switching costs
5. Access to distribution channels
6. Cost disadvantages independent of scale
7. Government policy

(B) Rivalry among Existing Firms Rivalry tactics include price competition, advertising battles, new product introduction, and increased customer service or product/service warranties. Competitors are mutually dependent in terms of action and reaction, moves and countermoves, or offensive and defensive tactics. Intense rivalry is the result of a number of interacting structural factors, such as numerous or equally balanced competitors, slow industry growth, high fixed costs or storage costs, lack of differentiation or switching costs, capacity increased in large increments, diverse competitors, high strategic stakes, and high exit barriers. Porter referred to the "advertising slugfest" when describing the scrambling and jockeying for position that often occurs among fierce rivals within an industry.[2]

PORTER'S COMPETITIVE FORCES AND COMPETITIVE STRATEGIES

Porter's five competitive forces include: (1) threat of new entrants, (2) rivalry among existing firms, (3) pressure from substitute products or services, (4) bargaining power of buyers, and (5) bargaining power of suppliers.

Porter's three competitive strategies include: (1) differentiation, (2) low-cost leadership, and (3) focus.

(C) Pressure from Substitute Products or Services In a broad sense, all firms in an industry are competitors with industries producing substitute products. Substitutes limit the potential returns of an industry by placing a ceiling on the prices firms can profitably charge. The more attractive the price–performance alternative offered by substitutes, the stronger or firmer the lid on industry profits. Substitute products that deserve the most attention are those that are subject to trends improving their price–performance trade-off with the industry's product or produced by industries earning high profits.

(D) Bargaining Power of Buyers Buyers compete with the industry by forcing down prices, bargaining for higher quality or more services, and playing competitors against each other—all at the expense of industry profits. A buyer group is powerful if these circumstances hold true:

- It is concentrated or purchases large volumes relative to seller sales.
- The products it purchases from the industry represent a significant fraction of the buyer's costs or purchases.
- The products it purchases from the industry are standard or undifferentiated.
- It faces few switching costs.
- It earns low profits.
- Buyers pose a credible threat of backward integration.

[2] Ibid.

- The industry's product is unimportant to the quality of the buyers' products or services.
- The buyer has full information about demand, prices, and costs.

Informed customers (buyers) become empowered customers.

(E) Bargaining Power of Suppliers Suppliers can exert bargaining power over participants in an industry by threatening to raise prices or reduce the quality of purchased goods or services. The conditions making suppliers powerful tend to mirror those making buyers powerful. A supplier group is powerful if these attributes apply:

- It is dominated by a few companies and is more concentrated than the industry it sells to.
- It is not obligated to contend with other substitute products for sale to the industry.
- The industry is not an important customer of the supplier group.
- The suppliers' product is an important input to the buyer's business.
- The supplier group's products are differentiated or it has built up switching costs.
- The supplier group poses a threat of forward integration.

(ii) Porter's Competitive Strategies

Porter studied a number of businesses and introduced a framework describing three generic competitive strategies to outperforming other firms in an industry. These strategies include differentiation, low-cost leadership, and focus. The focus strategy, in which the organization concentrates on a specific market or buyer group, is further divided into *focused low cost* and *focused differentiation.* This yields four basic strategies, and to use this model, managers evaluate two factors: competitive advantage and competitive scope. With respect to advantage, managers determine whether to compete through lower cost or through the ability to offer unique or distinctive products and services that can command a premium price. Managers then determine whether the organization will compete on a broad scope (in many customer segments) or a narrow scope (in a selected customer segment or group of segments). These choices determine the selection of strategies.

COMPETITIVE STRATEGY ACTIONS

Competitive strategy is taking offensive or defensive actions to create a defendable position in an industry to cope with the five competitive forces in order to achieve a superior return on investment (ROI).

The **differentiation** strategy involves an attempt to distinguish the firm's products or services from others in the industry. An organization may use advertising, distinctive product features, exceptional service, or new technology to achieve a product that is perceived as unique. This strategy usually targets customers who are not particularly concerned with price, so it can be quite profitable. The differentiation strategy can be profitable because customers are loyal and will pay high prices for the product. Companies that pursue a differentiation strategy typically need strong marketing abilities, a creative flair, and a reputation for leadership.

A differentiation strategy can reduce rivalry with competitors and fight off the threat of substitute products because customers are loyal to the company's brand. However, companies must remember that successful differentiation strategies require a number of costly activities, such as product R&D and extensive advertising.

With a **low-cost leadership** strategy, the organization aggressively seeks efficient facilities, pursues cost reductions, and uses tight cost controls to produce products more efficiently than competitors. A low-cost position means that the company can undercut competitors' prices and still offer comparable quality and earn a reasonable profit. Being a low-cost producer provides a successful strategy to defend against the five competitive forces. For example, the most efficient, low-cost company is in the best position to succeed in a price war while still making a profit. Likewise, the low-cost producer is protected from powerful customers and suppliers, because customers cannot find lower prices elsewhere, and other buyers would have less slack for price negotiation with suppliers. If substitute products or potential new entrants occur, the low-cost producer is better positioned than higher-cost rivals to prevent loss of market share. The low price acts as a barrier against new entrants and substitute products.

The low-cost leadership strategy tries to increase market share by emphasizing low cost compared to competitors. This strategy is concerned primarily with stability rather than taking risks or seeking new opportunities for innovation and growth.

With Porter's third strategy, the **focus** strategy, the organization concentrates on a specific regional market or buyer group. The company uses either a differentiation or low-cost approach, but only for a narrow target market.

Managers think carefully about which strategy will provide their company with its competitive advantage. In his studies, Porter found that some businesses did not consciously adopt one of these three strategies and were stuck with no strategic advantage. Without a strategic advantage, businesses earned below-average profits compared with those that used differentiation, cost leadership, or focus strategies. In addition, because the Internet is having such a profound impact on the competitive environment in all industries, it is more important than ever for companies distinguish themselves through careful strategic positioning in the marketplace.

These three approaches require different styles of leadership and can translate into different corporate cultures. A firm that is stuck in the middle is the one that has failed to develop its strategy in at least one of the three directions. The firm stuck in the middle has low profitability, lost high-volume customers, lost high-margin businesses, blurred corporate culture, and conflicting motivational systems. Risks in pursuing the three generic strategies are failing to attain or sustain the strategy and eroding the strategic advantage with industry evolution.

(ii) Competitive Analysis

The objective of a competitive or competitor analysis is to develop a profile of the nature and success of the likely strategy changes, each competitor's response to the strategic moves, and each competitor's probable reaction to the industry changes. A series of what-if questions must be raised and answered here.

There are four diagnostic components to a competitor analysis:

1. Future goals
2. Current strategy (either explicit or implicit)
3. Assumptions
4. Capabilities (strengths and weaknesses)

Both future goals and assumptions jointly answer this question: What drives the competitor? Both current strategy and capabilities jointly answer this question: What is the competitor doing, and what can it do?

Future goals should focus on attitude toward risks, financial goals, organizational values or beliefs, organizational structure, incentive systems, accounting systems, leadership styles, composition of the board of directors, and contractual commitments (debt covenants, licensing, and joint ventures).

Examining the assumptions can identify biases or blind spots that may creep into management thinking. Rooting out these blind spots can help the firm identify competitive moves or retaliation. Assumptions focus on competitors' relative position in cost, quality, and technology; cultural, regional, or national differences; organizational values; and future demand and industry trends.

A competitor's goals, assumptions, and current strategy will influence the likelihood, timing, nature, and intensity of a competitor's reactions. A competitor's strengths and weaknesses (i.e., capability) will determine its ability to initiate or react to strategic moves and to deal with industry events that occur.

(iii) Market Signals

A market signal is any action or indirect communication by a competitor that provides a direct or indirect indication of its intentions, motives, goals, or internal situation. The behavior of competitors provides several signals, such as bluffs, warnings, and earnest commitments. Market signals, either conscious or unconscious, can aid in competitor analysis and strategy formulations, where they add greatly to the firm's base of knowledge about competitors.

(iv) Industry Evolution

Analyzing industry evolution can increase or decrease the basic attractiveness of an industry as an investment opportunity, and it often requires the firm to make strategic adjustments. Structural analysis of industries is the starting point for analyzing industry evolution. Most of all, industry evolution should not be viewed as a fait accompli to be reacted to but as an opportunity to explore.

Some analytical techniques that will aid in anticipating the pattern of industry changes are listed next.

- Product life cycle
- Initial structures (the entry barriers, buyer power, and supplier power)
- Incentives or pressures for change
- Potential structures
- Long-run changes in industry growth
- Changes in buyer segments
- Buyers' knowledge about a product or service
- High degree of experimentation due to reduction of uncertainty about market size, optimal product configuration, and nature of buyers

- Diffusion of proprietary technology (patents)
- Accumulation of experience (learning curve)
- Expansion or contraction in scale
- Changes in input costs, such as wages, materials, cost of capital, media, and transportation
- Innovations in product, marketing, and process management
- Entry and exit barriers
- Structural changes in adjacent industries
- Changes in government policy

Industry evolution is similar to a product life cycle (the grandfather concept), where industry growth follows an S-shape curve due to innovation. Industry evolution has four stages: introduction, growth, maturity, and decline. The introductory phase is flat in terms of overcoming buyer inertia and stimulating trials of the new product. Rapid growth occurs as many buyers rush into the market once the product has proven successful. The maturity stage is reached when growth stops and levels off. Finally, growth will decline as new substitute products appear in the market.

Some criticism about the product life cycle concept are listed next.

- The duration of the stages varies widely from industry to industry, and it is often not clear what stage of the life cycle an industry is in.
- Industry growth does not always go through the S-shape pattern; some industries skip introduction or maturity, and some industries become active after decline.
- Product life cycles show one pattern of evolution when in fact several patterns can take place.

An industry is an interrelated system. As such, changes in one element of an industry's structure tend to trigger changes in other areas. Some key relationships in industry evolution are listed next.

- Industry concentration and mobility barriers move together.
- No concentration takes place if mobility barriers are low or falling.
- Exit barriers deter consolidation.
- Long-run profit potential depends on future structure.
- Structural change in an industry is often accompanied by changes in industry boundaries. Innovations in technology, product substitutes, and reduction in costs are enlarging the industry base by placing more firms in direct competition. This, in turn, changes the industry boundaries where suppliers and buyers compete with each other rather than work together.
- A firm's strategic behavior can change the industry structure. A company should be sensitive to external forces that can cause the industry to evolve. These forces include:
  - Specific forms of regulatory changes.
  - Diffusion of technological innovations.
  - Improvement in the cost or supply of complementary products.

(d) Industry Environments

In this section, competitive strategies related to fragmented industries, emerging industries, and declining industries are discussed. In addition, competition in global industries is presented, including sources and impediments, evolution of global markets, strategic alternatives, and trends affecting competition. This section is adapted from Porter's book titled *Competitive Strategy.*[3]

(i) Competitive Strategies Related to Fragmented Industries

A fragmented industry is defined as an industry where there is no single firm with a significant market size, where there are large numbers of small- and medium-size firms, and where there are no market leaders with the power to shape the industry events. These industries range from high tech to low tech, providing differentiated to undifferentiated products.

Although there is no fundamental economic basis for fragmentation, underlying economic causes for fragmentation include:

- Low entry barriers
- Absence of economies of scale or experience curve
- High transportation costs
- High inventory costs
- No significant bargaining power between buyers and suppliers
- Diverse market needs
- Economic and managerial exit barriers
- New industry
- Local regulations
- Government prohibition of concentration

Some industries are stuck in a fragmented state not because of fundamental economic reasons but because the existing firms lack resources or skills, are complacent, and lack attention by outside firms to infuse resources for consolidation.

The payoff to consolidating a fragmented industry can be high because the costs of entry into it are low, competition is weak, and there is little threat of retaliation. Common approaches to overcoming fragmentation that basically unlock the fundamental economic factors are listed next.

- Create economies of scale or experience curve (innovation).
- Standardize diverse market needs.
- Split off businesses that are responsible for fragmentation (i.e., decouple production from the rest of the business, use multiple in-house labels).
- Acquire many local companies.
- Recognize industry trends early.

[3] Ibid.

Profitability in the fragmented industry is marginal at best. Strategic positioning is needed to become a successful firm. Strategic alternatives for coping with a fragmented structure are listed next.

- Manage the decentralization organization structure tightly.
- Build low-cost, efficient facilities at multiple locations.
- Increase the value added of the business by forward integration (from manufacturing into distribution or retailing), specialization by product type, product segment, customer type, or order type.
- Focus on a geographic area.
- Maintain low overhead cost, tight cost control, low-skilled employees, and attention to detail.
- Practice selective backward integration to lower costs and to put pressure on competitors.

The strategic analyst should note these red flags (traps) during the analysis of strategic alternatives:

- Seeking dominance
- Lack of strategic discipline
- Overcentralization
- Incorrect assumptions about competitors' overhead costs and objectives
- Overreactions to new products that result in increasing overall costs and overhead costs

(ii) Competitive Strategies Related to Emerging Industries

Emerging industries (e.g., video games, solar heating, wind tunnel energy and fiber optics) are defined as newly formed or re-formed industries that have been created by technological innovations, shifts in cost structures, new consumer needs, and redefining the business due to growth in scale. Because there are no rules of the game to follow, they must be established. The absence of rules is both a risk and opportunity, which must be managed and explored, respectively.

Emerging industries, although they are small in size and new to the industry, possess common structural characteristics, such as technological and strategic uncertainty, high initial costs with steep learning curves, first-time buyers with the possibility of inducing substitution, short-term horizon to develop products and customers, and subsidization to early entrants from government and nongovernment sources.

Emerging industries usually face problems in getting off the ground. These problems include:

- Inability to obtain raw materials and components
- Period of rapid escalation of raw materials prices
- Absence of infrastructure, such as distribution channels and service facilities
- Absence of product or technological standardization
- Perceived likelihood of obsolescence
- Customer confusion

- Erratic product quality
- Image and credibility difficulties with the financial community
- Regulatory approval delays
- High unit costs
- Response of threatened entities, such as labor unions or distribution channels

The structure of an emerging industry is unsettled and changing, and competitors are hard to diagnose. Yet emerging industries can benefit from the strategic degrees of freedom and leverage from good strategic choices. Possible actions include:

- Shaping the industry structure
- Establishing industry conferences and trade associations
- Changing the role of suppliers and distribution channels
- Shifting mobility barriers requiring capital commitments where customers or suppliers are integrating into the industry

Common early mobility barriers include proprietary technology, access to distribution channels, access to raw materials, and risk, which raises the opportunity cost of capital and thereby increases effective capital barriers.

A crucial strategic choice for competing in emerging industries is the appropriate timing of entry. Early entry involves high risk, low entry barriers, and a large return. Early entry is appropriate when a learning process is initiated, customer loyalty is promising, and cost advantage is absolute. Early entry is not appropriate when costs of opening up the market are great, early competition is costly, technological change can make early investments obsolete, and the wrong human skills are built.

An emerging industry is attractive if its ultimate structure (not its initial structure) earns above-average returns. The decision to enter must depend on a structural analysis and a variety of scenarios. Different scenarios need to be developed for each product/technology/market combination and then utilized to forecast the probable success of different competitors. The firm may choose to try to cause the most advantageous scenario to occur and identify the key events, which will signal whether one scenario or another is actually occurring.

(iii) Competitive Strategies Related to Declining Industries

Declining industries are those industries experiencing an absolute decline in unit sales over a long period. The decline cannot be due to changes in business cycles or short-term problems, such as strikes or material shortages. Declining industries are characterized by shrinking sales and profit margins, pruning product lines, falling R&D efforts, reduced advertising budgets, and diminishing number of competitors. The decline phase of an industry is different from and more complex than the decline phase of a product life cycle. Industries differ markedly in the way competition responds to decline; some industries age gracefully and some engage in bitter warfare, all leading to prolonged excess capacity and heavy operating losses. M&A can reduce excess capacity and wipe out obsolete capacity. End-game strategies must be developed for declining industries.

Structural determinants of competition in declining industries are listed next.

- Conditions of demand, such as uncertainty, rate, and pattern of decline
- Causes of decline due to technological substitution, demographic changes, and shifts in customers' (buyers') needs
- Presence of exit barriers due to fixed assets and fixed costs
- Presence of strategic exit barriers, such as interrelatedness, vertical integration, and the ability to attract (access) financial markets
- Information barriers
- Managerial barriers (a blow to manager's pride, job mobility)
- Government and social barriers (unemployment)
- Price wars among competitors

There are four alternative strategies for declining industries, including: (1) leadership, (2) niche, (3) harvest, and (4) quick divestment. The **leadership strategy** assumes that the remaining firms have the potential to reap above-average profits and the leadership style is strong enough to keep up with competitors and to gain market share. Some tactical actions contributing to executing the leadership strategy are listed next.

- Investing in aggressive pricing and marketing
- Acquiring competitors or their product lines
- Purchasing or retiring competitors' capacity
- Reducing competitors' exit barriers by manufacturing spare parts
- Taking over long-term contracts and producing private label products
- Reinvesting in new products
- Making process improvements.

The objective of **niche strategy** is to create or defend a strong position in a particular segment. The structural characteristics include maintaining a stable demand or decaying slowly, and allowing high returns. The strategic actions include reducing competitors' exit barriers or reducing uncertainty concerning this segment. The firm may switch to a harvest or a divest strategy.

In the **harvest strategy,** the firm seeks to optimize cash flows from the business similar to the "dog" category in the product portfolio planning techniques. It does this by increasing prices, eliminating or reducing new investment, cutting maintenance of facilities, and reducing advertising and R&D budgets. It also reduces the number of product models and distribution channels; eliminates small customers; and reduces postsale services, such as delivery, repair, and customer service. Price increases and lower advertising actions are visible to the customer, while deferred maintenance and dropping marginal accounts and small customers are invisible to the customer. The accepted strategy for an industry in decline is a harvest strategy, that is, eliminating investment and generating maximum cash flows followed by divestment. The harvest strategy puts a greater demand on administrative matters due to problems such as low employee morale and retention, loss of suppliers' and customers' confidence, and questionable motivation of management.

In the **quick divestment strategy,** the firm sells (liquidates) the business early in the decline phase rather than harvesting and selling it later. This approach maximizes the value of the firm and minimizes potential risk due to incorrect forecast of future demand. It may be desirable for some firms to divest the business before decline to facilitate a stronger bargaining position. Divesting quickly may force the company to confront exit barriers, such as image, and interrelationships with suppliers and customers. The firm can use a private label strategy or sell product lines to competitors to solve exit barrier problems.

When the industry structure is favorable for decline because of low uncertainty and low exit barriers for competitors, the firm should use (1) the leadership or niche strategies if it has strengths relative to its competitors or (2) the harvest or divest-quickly strategies if it lacks strengths relative to its competitors.

When the industry structure is unfavorable for decline because of high uncertainty and high exit barriers for competitors, the firm should use (1) niche or harvest strategies if it has strengths relative to its competitors or (2) the divest-quickly strategy if it lacks strengths relative to its competitors.

A firm can make an early commitment to one decline strategy or another. An early commitment to leadership may encourage a competitor to exit; divestment can maximize the value of the firm. However, postponing a choice of decline strategy can force the firm toward either the niche or harvest strategy, thus eliminating the polar options of leadership or divest quickly. If the leading competitor decides to exit, the firm can invest; if the leading competitor stays, the firm can continue to harvest or divest quickly.

There should be consistency between industry structure and strategic choice a firm makes. The strategic analyst should keep these pitfalls in mind: failing to recognize decline and not participating in the substitute industry, warfare with competitors having high exit barriers leading to disaster, and harvesting without clear strengths.

A firm should prepare for the decline phase by taking three steps during the maturity phase: (1) minimize investments that raise exit barriers, (2) emphasize market segments that will be favorable under decline conditions, and (3) create high switching costs in these segments.

(iv) Sources and Impediments to Global Competition

Global industries require a firm to compete on a worldwide, coordinated basis. To analyze competition in a global industry, it is necessary to examine industry economics and competitors in the various geographic or national markets jointly rather than individually. Industries with multinational competitors are not necessarily global industries since "globalness" is a matter of degree.

The structural factors (cost differences, different circumstances, different roles of foreign governments, and different goals) and market forces operating in global industries are the same as those in domestic industries. Structural analysis in global industries must encompass foreign competitors, a wider pool of potential entrants, and a broader scope of possible substitutes. Firms can participate in international activities through three mechanisms, including export, licensing, and foreign direct investment, in that order. Export or foreign direct investment is present in industries where competition is truly global.

Sources of global competitive advantage include comparative advantage, economies of scale in production, logistics, marketing and purchasing areas, global experience, product differentiation,

proprietary product technology, and mobility of production. Note that all the sources of advantage also create mobility barriers for global firms.

Impediments to achieving the global competitive advantage include economic impediments, such as transportation and storage costs, differing product needs, sales force, distribution channels, local repair, sensitivity to lead times, complex price–performance trade-offs among competing brands, and lack of worldwide demand. Global competitive advantage can also be affected by managerial impediments, such as differing marketing tasks; intensive local services; rapidly changing technology; government impediments (including tariffs, duties, quotas, and local content requirements) and policies related to tax, labor, and bribery; and resource impediments, such as building world-scale facilities or start-up investments.

These impediments can block an industry from becoming a global industry altogether from cost and complexity viewpoints. Because of this, aspects of localness may remain even in industries that are truly global. In some markets, the national firm is better situated than the global firm due to localness.

(v) Evolution of Global Markets

Many industries evolve into global industries slowly over time. To create a global industry, a firm needs more sources of global competitive advantage or fewer impediments to global competition.

Environmental triggers to globalization include increased scale economies, decreased transportation or storage costs, increased factor costs (e.g., labor, energy, and materials), and reduced government constraints (e.g., tariffs, quotas, duties, taxes, and local content requirements).

Strategic innovations stimulating globalization are listed next.

- Redefinition of product
- Identification of market segments
- Reduced cost of product adaptations
- Product design changes toward standardized components
- De-integration of products where components are produced centrally and assembled locally
- Allowing new firms to start fresh with new strategies

(vi) Strategic Alternatives to Compete Globally

A firm must make a choice about whether it must compete globally or compete in one or a few national markets. The alternatives include broad-line global competition with a full product line, global focus (low cost or differentiation), national focus (low cost or differentiation), and protected niche, such as requiring high local content in the product and high tariffs. A better approach is to form transnational coalitions or cooperative agreements between firms in the industry that are located in different home countries.

(vii) Trends Affecting Global Competition

A number of trends greatly affect competition in existing global industries. These trends are listed next.

- Reduction in economic differences among countries, where differences among developed and newly developed countries (NDCs) are narrowing in terms of income, factor costs (e.g., labor, energy, and materials), marketing practices, and distribution channels.
- Adoption of a more aggressive industrial policy. Industrial policies of many countries are changing from passive postures to aggressive postures in order to stimulate industry in carefully selected sectors of the economy.
- Increasing protection of natural resources, such as oil, coal, and rubber. These assets have been controlled either directly by national government ownership or through joint ventures of governments and producers. These governments recognize the advantages of low-waged, semiskilled, and unskilled labor.
- Free flow of technology. Some countries have become very aggressive in selling their technology abroad or reselling it to others at bargain prices.
- Gradual emergence of new large-scale markets. Brazil, China, Russia, and India are becoming major global powers.
- Growing NDC competition. Cheap labor and natural resources as well as investments in capital-intensive industries are causing increased competition. Those industries most vulnerable to NDC competition are those that lack these entry barrier factors:
  - Rapidly changing proprietary technology
  - Highly skilled labor
  - Sensitivity to lead times
  - Complex distribution channels
  - High consumer marketing content
  - Complex and technical selling tasks

  These factors have become difficult problems for NDC firms to solve due to lack of resources or skills, inexperience, lack of credibility, or inability to understand distribution channels, consumer marketing, and complex selling taking place in the developed markets.

(e) Strategic Decisions

This section discusses integration strategies, capacity expansion, and entry into new businesses. This section is adapted from Porter's *Competitive Strategy.*[4]

(i) Analysis of Integration Strategies

Vertical integration is defined in terms of a firm exercising full control over the entire supply chain—that is, from purchasing of raw materials to production, distribution, and selling of goods or services. Vertical integration can occur in three ways: full integration (the entire supply chain done internally), partial (tapered) integration (part internally and part externally with independent contractors), and quasi integration (alliances or partnerships with other firms in the supply chain using debt or equity investment without full ownership). A firm can integrate either forward or backward, where the upstream firm is the selling firm and the downstream firm is the buying firm. It has been said that doing all of the vertical integration tasks internally is less costly, less risky, and easier to coordinate.

[4] Ibid.

FORWARD AND BACKWARD INTEGRATION

Forward integration means integrating activities from manufacturing to retailing activities. **Backward integration** means integrating activities from retailing to manufacturing activities. With forward integration, finished product prices can be raised. With backward integration, the cost of raw materials can be lowered.

Analysis of integration strategies requires not just the traditional cost/benefit analysis calculations but also more strategic, administrative, and marketing analysis. Integration analysis is similar to make-or-buy or purchase-or-lease decisions, as it focuses on economic or financial variables. The integration analysis should not focus on market transactions per se. Instead, it should balance the economic and administrative costs with economic and administrative benefits.

Strategic benefits of full integration are listed next.

- Economies of combined production where cost savings are achieved
- Economies of internal control and coordination through adjacent location of factories and distribution facilities
- Economies of information to obtain faster and accurate information about the marketplace
- Economies of marketing costs where there is no sales or purchasing staff
- Economies of stable relationship between upstream and downstream firms to develop efficient and specialized procedures
- Tapping into technology with the full understanding of technological risks involved
- Assurance of supply and demand to reduce uncertainty and risk of volatility with the use of internal transfer pricing methods
- Differentiation through better control of channels of distribution in order to offer better service to customers
- Raising mobility barriers to achieve higher prices, lower costs, or reduced risks
- Earning a higher ROI, more than the opportunity cost of capital
- Defending against foreclosure of access to suppliers or customers, which, in turn, raises the mobility barrier of access to distribution channels and suppliers of raw materials
- Offsetting bargaining power of suppliers or customers to lower the cost of raw materials (by backward integration) or to raise finished product prices (by forward integration) in order to operate more efficiently by eliminating non-value-added activities and practices

Strategic costs of full integration are listed next.

- Costs of overcoming mobility barriers due to cost of proprietary technology, favorable sources of raw materials, economies of scale, and capital requirements
- Increased operating leverage and business risk due to greater increase of fixed costs in the capital structure

- Reduced flexibility to change suppliers or customers due to increased cost of changeover
- Increased exit barriers
- Increased capital requirements with reduced flexibility in allocating investment funds
- Increased costs due to developing internal technological capability
- Costs of maintaining balance between upstream and downstream capacities of production, technological changes, and changes in product mix and quality
- Internal projects to expand capacity receiving less scrutiny than external contracts with customers or suppliers
- Indiscriminately applying the same organizational structure, managerial style, control and incentive systems, and capital budgeting techniques to upstream or downstream business units alike

Particular strategic issues to consider in **forward integration** (from manufacturing to retailing) are listed next.

- Improved ability to differentiate the product through better control of production process or sales process
- Increased mobility barriers due to improved differentiation; increased access to distribution channels
- Better access to market information in terms of quantity of demand, optimal product mix, and trends in customer tastes (referred to as demand leading stage) despite changing market conditions
- Realizing higher prices for products by setting different prices for different customers for the same product
- Locating the manufacturing plants in adjacent areas for greater economies of integration

Particular strategic issues to consider in **backward integration** (from retailing to manufacturing) are listed next.

- Avoiding sharing of proprietary data with suppliers due to internal production of parts or components
- Enhancing product differentiation by gaining control over the production of key input specifications
- Locating the manufacturing plants in adjacent areas for greater economies of integration

Partial (tapered) integration can take place either in the backward or forward direction, where some purchasing is done in the open market, which can be adjusted to reflect the degree of risk in the market. Partial integration results in lower fixed costs than full integration. In-house suppliers can be used to maintain steady production rates while independent suppliers can be used to handle the risk of market fluctuations. Partial integration reduces the risk of locked-in relationships with the suppliers and creates a healthy competition between in-house and independent suppliers. While using partial integration enables control over suppliers and leads to gains in knowledge regarding operating costs, it could increase coordination costs due to matching of external production with internal production.

Quasi integration falls in between the use of long-term contract suppliers and full ownership. Common integration arrangements can include minority equity investment, loan guarantees, specialized logistical facilities, and cooperative R&D work. Quasi integration can lower unit costs, reduce the risk of supply and demand interruptions, mitigate against bargaining power, and reduce the need to make full capital investment. These benefits stem from goodwill between partners, sharing of information, frequent and informal contacts between management, and the direct financial stake of each partner. However, some benefits, such as increasing ROI, raising product differentiation, and enhancing mobility barriers are difficult to achieve with quasi integration. A cost/benefit analysis is needed for each alternative arrangement in integration.

(ii) Capacity Expansion

For a manufacturing company, **capacity** is defined as the ability to produce a quantity of goods, as the market demands. Increasing capacity requires large amounts of capital investment, involves longer lead times, and is a complex decision-making process. Often capacity decisions are irreversible and can be compared to an economic oligopoly situation where firms are mutually dependent. Usually, the problem is overbuilding (overcapacity), not undercapacity. Prior to increasing capacity, a firm must have a clear expectation of future demand and competitors' behavior. However, the latter is difficult to predict. Overcapacity means supply is more than demand, while undercapacity means demand is greater than supply. Thus, capacity expansion deals with the uncertainty about future demand, which requires a systematic process. When the future demand is fairly certain, the capacity expansion process becomes a game of preemption. The risk of overbuilding is most severe in commodity-type businesses due to cyclical demand and undifferentiated products. M&A can reduce the excess capacity and wipe out the obsolete capacity.

Many conditions that can lead to overbuilding of capacity, including technological, structural, competitive, information flow, managerial, and governmental conditions. Each of these conditions is discussed next.

- Causes of overbuilding capacity due to technological conditions include: adding capacity in large lumps; long lead times in adding capacity; changes in production technology; and building new, efficient, and larger manufacturing plants.
- Causes of overbuilding capacity due to structural conditions include: significant exit barriers, forcing by suppliers, integrated competitors, firms striving for capacity leadership, and building credibility for new substitute products where customers take a wait-and-see approach.
- Causes of overbuilding capacity due to competitive conditions include: large number of firms, lack of credible market leaders, new entry, and first-mover advantages.
- Causes of overbuilding capacity due to information flow conditions include: overinflated future expectations about future demand, differing perceptions about competitor's strengths and resources, breakdown of market signals, industry structural changes, and pressure from the financial community to improve stock prices.
- Causes of overbuilding capacity due to managerial conditions include: production (not finance or marketing), orientation of management, and indifference between overbuilding and underbuilding of capacity.
- Causes of overbuilding capacity due to governmental conditions include: encouraging tax incentives, desire for indigenous industry, and pressure to increase or maintain employment.

There are limits to capacity expansion (overbuilding). These limits include:

- Financial constraints and company diversification, which increase the opportunity cost of capital
- Infusion of top management with finance backgrounds to replace marketing or production backgrounds
- Pollution control costs
- Uncertainty about future demand
- Capacity building costs
- Lessons learned from the past mistakes of overbuilding capacity

One approach to capacity expansion in a growing market is the preemptive strategy, where capacity is added in anticipation of future demand and prices are established in anticipation of future cost declines. The preemptive strategy discourages competitors from expanding and deters new entrants. This strategy is risky because of early commitment of resources before the market outcome is known. These conditions must be present for the preemptive strategy to be successful:

- Large capacity expansion relative to expected market size
- Large economies of scale relative to total market demand
- Credibility of the preempting firm
- Ability to signal preemptive motives before competitors act
- Willingness of competitors to back down due to high stakes in the market

Preemptive strategy are risky against competitors: with goals that are purely economicwith a strategic thrust, and that have equal or better staying power in the business (i.e., have a longer time horizon and are willing to trade profits for market position).

Three strategies exist to enter a new business: entry through internal development, entry through acquisition, and sequenced entry.

Entry through internal development requires building manufacturing facilities, distribution channels, and a sales force, or engaging in joint ventures. The internal entrant faces two entry barriers into an industry: structural entry barriers (proprietary technology, brand identification) and retaliation of existing firms (reduced prices, increased marketing costs, special promotions, extension of warranty terms, easier credit terms, and product quality improvements). Internal entrants increase the industry capacity by changing the supply and demand balance and triggering other firms in the industry to increase their capacity.

Internal entry is risky, costly, time consuming, and disruptive and provokes retaliation. Target firms that are risky to enter are those with slow growth, high fixed costs, high industry concentration, commodity-type products, and negative attitudes of the target firm's management.

Prime targets for internal entry by a firm are listed next.

- The industry is in disequilibrium (poor information and rising entry barriers).
- Slow retaliation from existing firms is expected.

- The firm has low entry costs due to increased mobility barriers and industry consolidation.
- The firm has unique qualities to influence the industry structure.
- The firm can create synergy with existing businesses.

Some common approaches or concepts to enter into a new business include:

- Reduce product costs
- Buy into the market with low initial prices
- Offer a superior, broad-based product
- Find a new niche
- Introduce a marketing innovation
- Use established distribution channels

Entry through acquisition, which is considered less costly and less time consuming than internal development, means buying other firm(s) in the industry for a price that is set in the marketplace. The acquisition market is active and efficient with many finders, brokers, and investment bankers who work to eliminate any above-average profits from an acquisition. A properly executed acquisition can reduce excess capacity or wipe out obsolete capacity.

An economic concept related to acquisition is that a seller will not sell a business unless the sale price exceeds the expected present value (floor) of continuing to operate the business. In reality, a large premium price over the market value is the rule rather than the exception in order to motivate the seller to sell the business. Acquisition will be profitable if the floor price is low, the market is imperfect (complex motives and incomplete information), and the buyer has a unique ability to manage the acquired business. Since the market for companies is imperfect, the bidding process will not completely eliminate profits from an acquisition. However, imperfection in the marketplace can lead to successful acquisition when:

- The buyer has superior information in terms of new technology and future demand.
- The number of bidders is low.
- The economy is bad.
- The selling company is "sick" (it is bought now at below-the-book value and is later sold for a profit).
- The buying firm has a good name and reputation in the industry in terms of retaining existing employees and management.
- The buyer has a unique ability to operate the seller's business.
- The new business fits well with the existing business.

Sequenced entry into a new business means that a buyer enters into one group of businesses first and later moves into other groups. This sequenced entry lowers the total cost of overcoming mobility barriers into the strategic business groups, which, in turn, lowers the overall risk. Other benefits of sequenced entry include developing managerial talent, tempered competitors' reactions, and accumulation of capital needed for subsequent acquisitions. The buying firm can then make reversible investments (salvageable or salable plant capacity) to overcome mobility

barriers. This means first starting with production operations and then moving into other areas, such as R&D, logistics, and marketing.

(f) Portfolio Techniques of Competitive Analysis

Portfolio strategy pertains to the mix of business units and product lines that fit together in a logical way to provide synergy and competitive advantage for the corporation. For example, an individual might wish to diversify in an investment portfolio with some high-risk stocks, some low-risk stocks, some growth stocks, and perhaps a few income bonds. In much the same way, corporations like to have a balanced mix of business divisions called **strategic business units (SBUs)**. An SBU has a unique business mission, product line, competitors, and markets relative to other SBUs in the corporation. Executives in charge of the entire corporation generally define the grand strategy and then bring together a portfolio of strategic business units to carry it out.

Portfolio models or techniques can help corporate management to determine how resources should be allocated among the various SBUs consisting of product lines and/or divisions. Portfolio techniques are more useful at the corporate-level strategy than at the business-level or functional-level strategy. Two widely used portfolio models are: the Boston Consulting Group (BCG) matrix and (2) the General Electric (GE) model. Each model is presented in the following sections.

(i) BCG Matrix Model

The BCG matrix model organizes businesses along two dimensions: business growth rate and market share. **Business growth rate** pertains to how rapidly the entire industry is increasing. **Market share** defines whether a business unit has a larger or smaller share than competitors. The combinations of high and low market share and high and low business growth provide four categories for a corporate portfolio.

The BCG matrix model utilizes a concept of experience curves, which are similar in concept to learning curves. The experience curve includes all costs associated with a product and implies that the per-unit cost of a product should fall, due to cumulative experience, as production volume increases. The manufacturer with the largest volume and market share should have the lowest marginal cost. The leader in market share should be able to underprice competitors and discourage entry into the market by potential competitors. As a result, the leader will achieve an acceptable ROI.

COMPETITIVE ADVANTAGE DEFINED

A firm is said to have a sustainable competitive advantage over other firms when it has technical superiority, low-cost production, good customer service/product support, good location, adequate financial resources, continuing product innovations, and overall marketing skills.

The BCG model (growth/market share matrix) is based on the assumption that profitability and cash flows will be closely related to sales volume. Here, growth means use of cash and market share means source of cash. Each SBU is classified in terms of its relative market share and the growth rate of the market the SBU is in, and each product is classified as stars, cash cows, dogs,

or question marks. Relative market share is the market share of a firm relative to that of the largest competitor in the industry.

The next list describes the components of the BCG model.

- **Stars** are SBUs with a high market share of a high-growth market. They require large amounts of cash to sustain growth despite producing high profits. Stars are important because they have additional growth potential, and profits should be plowed into this business as investment for future growth and profits. Stars are visible and attractive and will generate profits and a positive cash flow even as the industry matures and market growth slows. Stars eventually turn into cash cows as the market growth slows.
- **Cash cows** are often market leaders (high market share), but the market they are in is a mature, slow-growth industry (low growth). Because heavy investments in advertising and plant expansion are no longer required, the corporation earns a positive cash flow. It can milk the cash cow to invest in other, riskier businesses. Cash cows are used to turn question-mark SBUs into stars.
- **Dogs** are poorly performing SBUs that have a low market share of a low-growth market. They are modest cash users and need cash because of their weak competitive position. Dogs provide little profit for the corporation and may be targeted for divestment or liquidation if turnaround is not possible. Dog SBUs should be either harvested or divested from the portfolio.
- **Question marks** (wildcats) are SBUs with a low market share of a new, high-growth market. They require large amounts of cash inflows to finance growth and are weak cash generators because of their poor competitive position. The question-mark business is risky: It could become a star, or it could fail. The corporation can invest the cash earned from cash cows in question marks with the goal of nurturing them into future stars. SBUs not chosen for investment should be harvested (managed to generate cash) until they become dogs.

DESIRABLE SEQUENCE OF PORTFOLIO ACTIONS

- Cash-cow SBUs should be used to turn question marks into stars.
- A star SBU eventually becomes a cash cow as its market growth slows.
- Unqualified question-mark SBUs should be harvested until they become dogs.
- Dog SBUs should either be harvested or divested from the portfolio.
- Question-mark SBUs can be nurtured to become future stars.

WHICH MODEL IS WHICH?

- Both the BCG matrix and the GE model focus on corporate-level strategy accomplished through acquisition or divestment of business.
- Porter's five competitive forces and three competitive strategies focus on business-level strategy accomplished through competitive actions.

Despite its widespread use in allocating corporate resources and acceptance by managers, the BCG model has been criticized for:

- Focusing on market share and market growth as the primary indicators of profitability.
- Its assumption that the major source of SBU financing comes from internal means.
- Its assumption that the target market has been defined properly along with its interdependencies with other markets.

(ii) GE Model

The GE model is an alternative to the BCG model and incorporates more information about market opportunities (industry attractiveness) and competitive positions (company/business strength) to allocate resources. The GE model emphasizes all the potential sources of business strength and all the factors that influence the long-term attractiveness of a market. All SBUs are classified in terms of business strength (i.e., strong, average, weak) and industry attractiveness (i.e., high, medium, low).

The major components of industry attractiveness are market size, market share, market growth, industry profitability, and pricing. Business strength is made up of market share, quality leadership, technological position, company profitability, company strengths and weaknesses, and company image.

Overall strategic choices include either to invest capital to build position, to hold the position by balancing cash generation and selective cash use, or to harvest or divest. Because the GE model incorporates subjective judgment, it is vulnerable to manipulation. However, it can be made stronger with the use of objective criteria.

Both the BCG matrix model and the GE model help in competitive analysis and provide a consistency check in formulating a competitive strategy for a particular industry. Either model can be used as per the manager's preference. However, if a competitor uses the BCG model because of experience curves, then a company can benefit by using the same model.

(g) Forecasting

The simplest form of forecasting is the projection of past trends called extrapolation. Model building activities are examples of analytical techniques. A model breaks down a major problem into parts or subproblems and solves it sequentially. Some examples of applications of forecasting models in managerial accounting are pricing, costs, revenue, and inventory decisions.

For example, when forecasting purchases of inventory for a firm, factors such as knowledge of the behavior of business cycles, econometrics, and information on the seasonal variations in demand are important.

Models require a set of predetermined procedures. If there are no well-ordered and fully developed procedures, there is no need to model. That is, no procedure, no model. For example, a onetime crisis situation cannot be modeled due to lack of a preset procedure.

A key concept in all forecasting models dealing with probabilities is the expected value. The expected value equals the sum of the products of the possible payoffs and their probabilities.

(i) Time Series Analysis

Time series analysis is the process by which a set of data measured over time is analyzed. Decision makers need to understand how to analyze past data if they expect to incorporate past information into future decisions. Although the factors that affect the future are uncertain, often the past offers a good indication of what the future will hold. The key is to know how to extract the meaningful information from all the available past data.

All time series contain at least one of four time series components: long-term trend, seasonal, cyclical, and random or irregular components. Time series analysis involves breaking down data measured over time into one or more of these components. Time series analysis is similar to regression analysis in that both techniques help to explain the variability in data as much as possible. The four components of time series analysis help explain that variability (see Exhibit 5.3). The purpose of time series analysis is to use these components to explain the total variability in past data. The problem is how best to separate each component from the others so that each can be analyzed clearly.

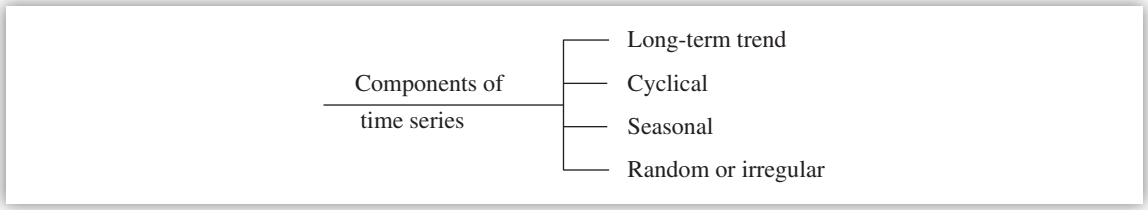


EXHIBIT 5.3 Components of Time Series

(A) Long-Term Trend The trend component is the long-term increase (growth) or decrease (decline) in a variable being measured over time. An example is annual sales over the past 10 to 15 years. Because long-term forecasting is becoming increasingly important due to severe global competition, the trend component in time series analysis is important to all organizations.

Long-term growth patterns have a wide variety of shapes, such as the first-degree, exponential, and Gompertz curves. The easiest method to fit trend lines to a series of data is to graph the data and draw the trend line freehand. Another way of fitting a trend line to a set of data is to use the least square regression method. *Two methods are available to fit a trend line to a series of data: (1) draw the trend line freehand, and (2) use the least square regression method.*

(B) Seasonal Component The seasonal component represents those changes in a time series that occur at the same time every year. An example is peak sales occurring once in the spring and once in the fall season.

Some organizations (e.g., toy stores, food processors, lumber mills) are affected not only by long-term trends but also by seasonal variations. The demand for products or services is highly dependent on the time of year. Those organizations that face seasonal variations are interested in knowing how well or poorly they are doing relative to the normal seasonal variation. The question is whether the increase or decrease is more or less than expected, or whether it occurs at more or less than the average rate.

A seasonal index known as the ratio to moving average can be calculated to measure seasonal variation in a time series. A 12-month moving average is used here. Seasonal variation affects the overall planning process, especially in labor requests, inventory levels, training needs, and periodic maintenance work.

Some prefer to eliminate irregular components in the data by taking the normalized average of the ratio to moving averages. A requirement prior to separating the irregular components from the data is to make sure that the ratio to moving averages is stable from year to year. Another assumption to be made prior to eliminating irregular components is that the irregular fluctuations are caused by purely random circumstances.

(C) Cyclical Component In addition to the seasonal component, data can contain certain cyclical effects. Cyclical effects in a time series are represented by fluctuations around a long-term trend. These fluctuations are thought to be caused by pulsations in factors such as interest rates, money supply, consumer demand, market conditions, and government policies. Cyclical fluctuations repeat themselves in a general pattern in the long term but occur with differing frequencies and intensities. Thus, they can be isolated but not totally predicted. Firms affected by cyclical fluctuations are those vulnerable to unexpected changes in the economy. The effect is different each time it occurs.

Cyclical variations in time series data do not repeat themselves in a regular pattern as do seasonal factors, but they cannot be considered random variations in the data either.

The organizations hardest hit by the cyclical component are those connected with items purchased with discretionary income (e.g., big-ticket items such as home appliances and automobiles). Because consumers can postpone purchasing these items, organizations that produce them are the most affected by a downturn in the economy.

The cyclical component is isolated by first removing the long-term trend and seasonal factors from the time series data. Then statistical normal values are calculated by multiplying the trend value by the seasonal index values. Finally, the cyclical component, which also contains the irregular component, is determined for each time period.

(D) Random or Irregular Component The random or irregular component is the one that cannot be attributed to any of the three components already discussed (long-term trend, seasonal, and cyclical components) (see Exhibit 5.4). Random fluctuations can be caused by many factors, such as economic failures, weather, political events.

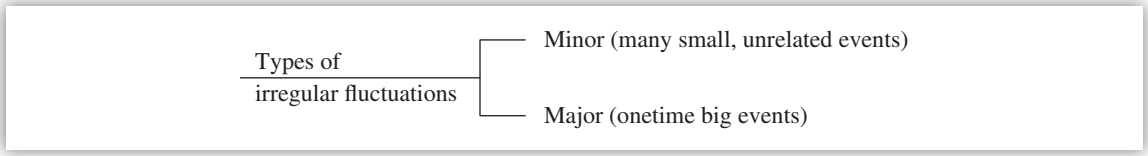


EXHIBIT 5.4 Types of Irregular Fluctuations

Minor irregularities show up as sawtooth-like patterns around the long-term trend. Individually they are not significant, but collectively they can be significant and could cause problems to many organizations.

LARGE VERSUS SMALL IRREGULAR VARIATIONS

- Large irregular variations cause greater problems.
- Small irregular variations cause lesser problems.

Major irregularities are significant onetime, unpredictable changes in the time series due to such extended and uncontrolled factors as a war, an oil embargo, a summer drought, or a severe winter storm.

Almost all industries and organizations are affected by irregular components. Agriculture, insurance, and mining companies will be more interested in this component. Minor irregularities can be smoothed out by using a moving average method. The goal is to eliminate as much as possible the irregular influences so that the true seasonal and cyclical components can be recognized and used. *A random component is unwanted. Buying insurance coverage is one way to mitigate the risks resulting from major irregular fluctuations.*

(ii) Regression Analysis

Regression analysis is a statistical technique used to measure the extent to which a change in the value of one variable, the independent variable, tends to be accompanied by a change in the value of another variable, the dependent variable.

Most measures of associations are nondirectional; that is, when calculated, it is not necessary to indicate which variable is hypothesized to influence the other. Measures of association show to what degree, on a 0-to-1 scale, two variables are linked.

DEFINITION OF KEY TERMS: REGRESSION ANALYSIS

- **Analysis of covariance.** A method of analyzing the differences in the means of two or more groups of cases while taking account of variation in one or more interval-ratio variables.
- **Analysis of variance.** A method for analyzing the differences in the means of two or more groups of cases.
- **Asymmetric measure of association.** A measure of association that makes a distinction between independent and dependent variables.
- **Auxiliary variable.** Another name for "independent variable."
- **Correlation.** A synonym for "association." Correlation is one of several measures of association. Correlation means the interdependence between two sets of numbers or a relation between two quantities, such that when one changes, the other changes. Simultaneous increasing or decreasing of quantities is called positive correlation; when one quantity increases while the other decreases, it is called negative correlation.
- **Dependent variable.** A variable that may, it is believed, be predicted by or caused by one or more other variables called independent variables. It will show the effect.
- **Discriminant analysis.** A tool for discriminating between effective and ineffective policies or procedures. It is based on subjective assessment (not based on statistics) and discrete values.
- **Explanatory variable.** Another name for "independent variable."
- **Independent variable.** A variable that may, it is believed, predict or cause fluctuation in a dependent variable.
- **Primary variable.** Another name for "dependent variable."
- **Regression.** The line of average relationship between the dependent (or primary) variable and the independent (or auxiliary) variable.

- **Regression analysis.** A method for determining the association between a dependent variable and one or more independent variables.
- **Regression coefficient.** A measure of change in a primary variable associated with a unit change in the auxiliary variable. An asymmetric measure of association; a statistic computed as part of a regression analysis.
- **Regression estimate.** An estimate of a population parameter for one variable that is obtained by substituting the known total for another variable into a regression equation calculated on the basis of the sample values of the two variables. Note that ratio estimates are special kinds of regression estimates.
- **Symmetric measure of association.** A measure of association that does not make a distinction between independent and dependent variables.

Managers often need to determine the relationships between two or more variables prior to making a decision or for predicting and planning purposes or when analyzing a problem. When two variables are involved, simple linear regression and correlation analysis are the most often applied statistical tools for decision making. They provide a basis for analyzing two variables and their relationship to each other.

When more than two variables are involved, multiple regression analysis will be useful. Where only one independent variable is involved in the analysis, the technique is known as simple regression analysis; where two or more independent variables are involved, the technique is called multiple regression analysis (see Exhibit 5.5).

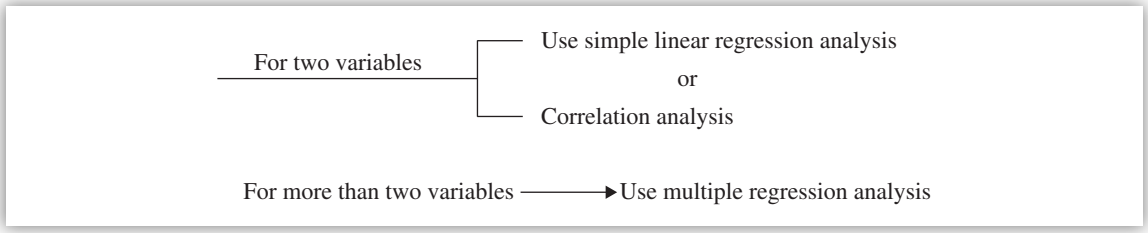


EXHIBIT 5.5 Simple Regression and Multiple Regression

The basic diagram, or scatter plots, can be used to depict potential relationships between a dependent variable *Y* (e.g., sales) and an independent variable *X* (e.g., advertising). The scatter plot provides a visual feel for the relationship between variables (qualitative measurement). A dependent variable is the variable whose variation is of interest. An independent variable is a variable used to explain variation in the dependent variable. The independent variable is also called an explanatory variable. Three possible relationships can emerge from the scatter plots: linear, curvilinear, and no relationship (see Exhibit 5.6).

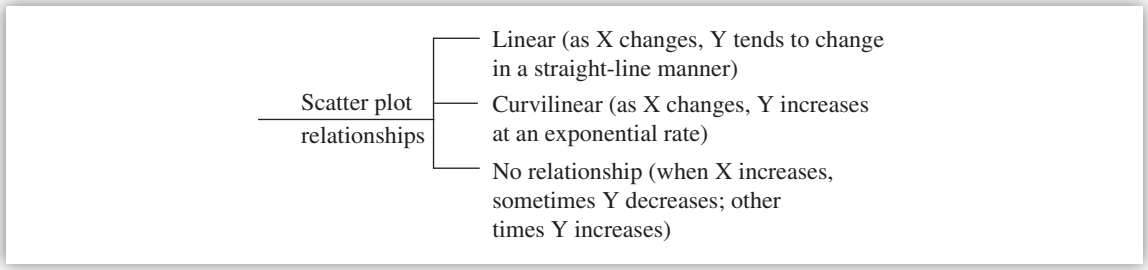


EXHIBIT 5.6 Scatter Plot Relationships

- **Linear.** As *X* changes, *Y* tends to change in a straight line or near straight-line manner. It can be positive change (*Y* increases as *X* increases) or negative change (*Y* decreases as *X* increases).
- **Curvilinear.** As *X* increases, *Y* increases at an exponential rate (example, as production increases, overtime is increasing at an exponential rate). As *X* increases, *Y* increases at a diminishing rate (e.g., when advertising is allowed to grow too large, diminishing returns will occur for sales).
- **No relationship.** When *X* increases, sometimes *Y* decreases; other times *Y* increases.

In addition to qualitative measure (i.e., visual feel), quantitative measurement using the correlation coefficient is needed to measure the strength between two variables. The correlation coefficient can range from a perfect positive correlation (+1.0) to a perfect negative correlation (–1.0). If two variables have no linear relationship, the correlation between them is 0. Consequently, the more the correlation differs from 0, the stronger the linear relationship between the two variables. The sign of the correlation coefficient indicates the direction of the relationship but does not aid in determining the strength.

Example

Given four values of correlation coefficient –0.15, –0.75, 0.19, and 0.35, which value indicates the weakest linear association between two variables?

Answer: The value –0.15 has the weakest linear association because it is farther from –1.0 than the other choices.

USES OF REGRESSION ANALYSIS

Two basic uses of regression analysis are as a descriptive tool and as a predictive tool. Some examples of using the **descriptive tool** are listed next.

- To describe the relationship between a loan's term (number of months) and its dollar value by a loan officer in a bank. A positive linear relationship might exist between time and amount in which smaller loans would tend to be associated with shorter lending periods whereas larger loans would be for longer periods.
- To explain the meaning of economy as viewed by economists.
- To describe the factors that influence the demand for products as presented by market researchers.

Some examples of using the **predictive tool** are listed next.

- To predict manufacturing production levels
- To forecast annual tax revenues
- To predict inventory levels

Determining whether the linear relationship between sales and advertising is significant requires us to test whether the sample data support or refute the hypothesis that the population correlation coefficient is 0. A *t* statistic is used to test the hypothesis that the population coefficient is 0.

The correlation does not imply cause and effect, since two seemingly unconnected variables often are highly correlated. When a correlation exists between two seemingly unrelated variables, the correlation is spurious at best. Even in the case of sales and advertising, one might be tempted to say that a cause and effect exist, but in reality there is no guarantee of a cause-and-effect (C&E) situation.

(A) Simple Linear Regression Analysis When the relationship between the dependent variable and the independent variable is a straight line (linear), the technique used for prediction and estimation is called the simple linear regression model. Exhibit 5.7 shows simple linear regression where the plotted data represents the heights of boys of various ages. The straight line represents the relationship between height (the dependent variable) and age (the independent variable) as disclosed by regression analysis. If the change in the dependent variable associated with a change in the independent variable does not occur at a constant rate, the relationship can be represented by a curved line and is referred to as curvilinear.

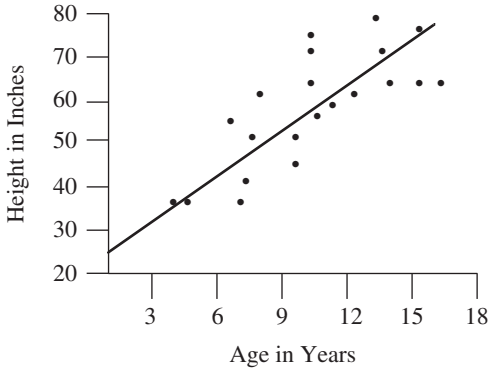


EXHIBIT 5.7 Simple Linear Regression

The simple linear regression model is represented by the next equation:

$$Yi = ß0 + ß1\ Xi + ei$$

where Yi = Value of the dependent variable
Xi = Value of the independent variable
ß0 = Y-intercept (a regression coefficient defining the true population model)
ß1 = Slope of the regression line (a regression coefficient defining the true population model)
ei = Error term or residual (a random component)

The random component is the difference between the actual Y value and the value of Y predicted by the model, and i could be positive or negative, depending on whether a single value of Y for a given X falls above or below the regression line. These ei values will have a mean of 0 and a standard deviation called the standard error of the estimate. If this standard error is too large, the regression model may not be very useful for prediction.

Here the regression model connects the averages of dependent variable Y for each level of independent variable X. The regression line, a straight line, is determined by two values, ß0 and ß1.

SIMPLE REGRESSION ANALYSIS

In simple regression analysis, the correlation coefficient measures the strength of the linear relationship between any two variables (X and Y); the analysis of variance "F" test indicates whether the regression model explains a significant proportion of variation in the dependent variable.

Managers would like to estimate the true linear relationship between dependent and independent variables by determining the regression model using sample data. A scatter plot can be drawn with the sample data to estimate the population regression line. The least squares criterion is used to select the best line since many possible regression lines exist for a sample of data. According to the least squares criterion, the best regression line is the one that minimizes the sum of squared distances between the observed (X,Y) points and the regression line. *Residual is the difference between the true regression line and the actual* Y *value.*

(B) Assumptions of the Simple Linear Regression Model The next list provides assumptions of the simple linear regression model.

- Individual values of the dependent variable, Y, are statistically independent of one another.
- For a given X value, there can exist many values of Y. Further, the distribution of possible Y values for any X value is normal.
- The distribution of possible Y values has equal variances for all values of X.
- The means of the dependent variable, Y, for all specified values of the independent variable can be connected by a straight line called the population regression model.

Some major considerations in using regression analysis as a predictive tool are listed next.

- Conclusions and inferences made from a regression line apply only over the range of data contained in the sample used to develop the regression line. The applicable range of data is called the relevant range of data. Any predictions beyond the relevant range of data lead to overpredictions. Thus, the range of data in the sample should cover the range of data in the population. Only then will a true relationship between the dependent variable and the independent variable emerge.
- A significant linear relationship existing between two variables does not imply that one variable causes the other. Although there may be a C&E relationship, managers should not infer the presence of such a relationship based only on regression and/or correlation analysis. Other factors, such as judgment, experience, and knowledge of the specific area of interest, should also be considered.
- A C&E relationship between two variables is not necessary for regression analysis to be used for prediction. It is important to make sure that the regression model accurately reflects the relationship between the two variables and that the relationship remains stable.
- A high *coefficient of determination* (R^2) does not guarantee that the regression model will be a good predictor. The R^2 applies only to the sample data—measuring the fit of the regression line to the sample data—not to any other data.

The least squares regression line minimizes the sum of squared residuals. This value is called the sum of squares error (SSE). It represents the amount of variation in the dependent variable that is not explained by the least squares regression line; the amount of variation in the dependent variable that is explained by the regression line is called the sum of squares regression (SSR).

$$SSR = TSS - SSE$$

where TSS = Total sum of squares explaining the amount of total variation in the dependent variable

The percentage of the total variable in the dependent variable that is explained by the independent variable is called the coefficient of determination (R^2). R^2 can be a value between 0 and 1.0. R^2 indicates how well the linear regression line fits the data points (X,Y). *The better the fit, the closer R^2 will be to 1.0.*

INTERPRETATION OF R^2

- R^2 is 1.0 when there is a perfect linear relationship between two variables.
- R^2 will be close to zero when there is a weak linear relationship or no linear relationship at all.

When R^2 is 1.0, it corresponds to a situation in which the least squares regression line would pass through each of the points in the scatter plot. Least square criterion ensures that R^2 will be maximized. R^2 applies only to the sample data used to develop the model.

APPLICATION OF REGRESSION ANALYSIS

Example 1

XYZ Company derived the following cost relationship from a regression analysis of its monthly manufacturing overhead cost.

$$C = \$80{,}000 + \$12\ M$$

where C = Monthly manufacturing overhead cost
M = Machine hours

The standard error of estimate of the regression is $6,000. The standard time required to manufacture a case of the company's single product is four machine hours. XYZ applies manufacturing overhead to production on the basis of machine hours, and its normal annual production is 50,000 cases.

Question: What is the estimated variable manufacturing overhead cost for a month in which scheduled production is 5,000 cases?

Answer: In the cost equation C = $80,000 + $12 M, $80,000 is the fixed cost component and $12M is the variable cost component. That is, $12 × 5,000 cases × 4 machine hours per case = $240,000.

Question: What is the predetermined fixed manufacturing overhead rate?

Answer: Since $80,000 is the fixed component per month, we need to multiply this by 12 to obtain one year fixed cost. The predetermined overhead rate per machine hour is ($80,000 × 12)/(50,000 × 4) = $4.80.

Example 2

The linear regression equation, Y=15.8 + 1.1(x), was used to prepare the next data table.

Actual X	*Predicted* Y	*Actual* Y	*Residual*
0	15.8	10	–5.8
1	16.9	18	1.1
2	18.0	27	9.0
3	19.1	21	1.9
4	20.2	14	–6.2

Question: What do you conclude from the data table?

Answer: The best description of the data is that the relationship is not linear. A linear equation was used with nonlinear relationship. If the relationship was linear, the results of actual *Y* would have been higher than or equal to 15.8; it is not. Two values (10 and 14) are less than 15.8, indicating a nonlinear relationship.

(C) Multiple Regression Analysis Regression analysis is used for prediction and description to determine the relationship between two or more variables. The multiple regression analysis technique analyzes the relationship between three or more variables and is an extension of simple regression analysis. *In simple regression analysis, there is only one independent variable. In multiple regression analysis, there is more than one independent variable.* Exhibit 5.8 presents a comparison between simple regression and multiple regression analysis.

Characteristics of simple regression	Characteristics of multiple regression
Sales is a dependent variable and advertising expenditures is an independent variable.	House price is a dependent variable. Square feet of house, age of house, number of bedrooms, and number of bathrooms are examples of independent variables.
The model is an equation for a straight line in a two-dimensional space.	The model forms a hyperplane through multidimensional space.
Each regression coefficient represents a slope and involves a matrix algebra.	Each regression coefficient represents a slope and involves a matrix algebra.
Can use graph or calculator to solve the problem. Use of computer is optional.	Must use computer to solve the problem.
The correlation coefficient is calculated.	The correlation matrix is calculated.

EXHIBIT 5.8 Comparison between Simple Regression and Multiple Regression

From a theoretical viewpoint, the sample size required to compute a regression model must be at least one greater than the number of independent variables; that is, for a model with four independent variables, the absolute minimum number of case samples required is five. Otherwise, the model will produce meaningless values. From a practical standpoint, the sample size should be at least four times the number of independent variables.

SIMPLE REGRESSION VERSUS MULTIPLE REGRESSION

- When there are two variables (one dependent and one independent), we call it a bivariate or simple regression.
- When there are more than two variables (one dependent and more than one independent), we call it a multivariate or multiple regression.
- The multivariate model offers a better fit than the bivariate model.

(D) Assumptions of the Multiple Regression Model The next list provides assumptions about the multiple regression model.

- The errors are normally distributed.
- The mean of the error terms is zero.

- The error terms have a constant variance for all combined values of the independent variables.

In multiple regression analysis, additional independent variables are added to the regression model to explain some of the yet-unexplained variation in the dependent variable. Adding appropriate additional variables would reduce the standard error of the estimate where the value of the latter is too large for the regression model to be useful for prediction.

The *correlation matrix* is useful for determining which independent variables are likely to help explain variation in the dependent variable. A value of ± 1.0 indicates that changes in the independent variable are linearly related to changes in the dependent variable.

Similar to simple regression, multiple regression uses R^2, the multiple coefficient determination, and is determined as follows:

$$R^2 = \frac{\text{Sum of squares regression}}{\text{Total sum of square}} = \frac{\text{SSR}}{\text{TSS}}$$

Example

If R^2 is 0.75, then 75% of the variation in the dependent variable can be explained by all independent variables in the multiple regression model.

When highly correlated independent variables are included in the regression model, a condition of overlapping called **multicollinearity** can exist. Specifically, when two independent variables are correlated with each other, adding redundant information to the model, multicollinearity does exist in practice. The best practical advice is to drop the independent variable(s) that is the main cause of the multicollinearity problems from the model.

Multicollinearity influences the regression model negatively—the regression coefficient sign is the opposite of the expected sign. The independent variable causing multicollinearity is not necessary to the functioning of the model and hence can be removed without any loss. It is highly correlated with other independent variables and has low correlation with the dependent variable.

(E) Symptoms of Multicollinearity in Regression The next list provides symptoms of multicollinearity in regression analysis:

- Incorrect signs on the coefficients
- A change in the values of the previous coefficients when a new variable is added to the model
- The change to insignificant of a previously significant variable when a new variable is added to the model
- An increase in the standard error of the estimate when a variable is added to the model

Not all independent variables contribute to the explanation of the variation in a dependent variable. Some variables are significant, but not all. *The significance of each independent variable can be tested using a "t" test. It is calculated by dividing the regression coefficient by the standard deviation of the regression coefficients.*

"F" TEST VERSUS "t" TEST

- The "F" test is used to explain the significance of just one independent variable.
- The "t" test is used to explain the significance of each independent variable. Multicollinearity affects the "t" test.

The regression model used for prediction should contain significant independent variables only. If insignificant variables exist, they should be removed and the regression model rerun before it is used for prediction purposes. Any coefficient with an unexpected sign indicates a problem condition. Unexpected sign implies unreasonable relationships between variables.

Developing a multiple regression model is an art. Judgment is required when selecting the best set of independent variables for the model that are less in conflict and contribute to the best predictor.

(F) Dummy Variables in Regression Models When an independent variable in a regression model is a nominal or ordinal variable, it is called a qualitative variable. For example, in a model for predicting individual income, each manager may assign different values for a potential qualitative variable—for example, sex (male or female)—affecting the regression analysis.

In order to assign unique numerical values for these qualitative variables, dummy variables are added to the regression model. Rules for dummy variables include: If the qualitative variable has two possible categories (e.g., male or female), one dummy variable is added, and for more than two possible categories, one less than the number of possible categories is added (i.e., for five categories, only four dummy variables). Not following these rules would introduce unwanted multicollinearity and the fact that least squares regression estimates cannot be obtained if the number of dummy variables equals the number of possible categories. Dummy variables take on values of 0 and 1, and they represent the qualitative variables in the regression analysis.

(G) Regression Methods Basically, there are two methods for developing a regression model: ordinary regression and stepwise regression (see Exhibit 5.9).

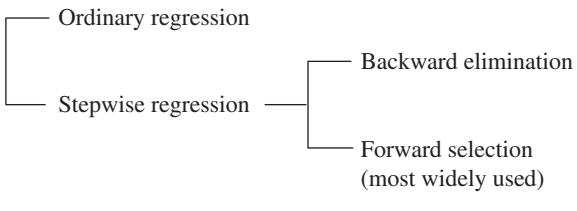


EXHIBIT 5.9 Regression Methods

In the **ordinary regression method,** all independent variables are brought into the model at one step. The **stepwise regression method** develops the least squares regression equation in steps, through either backward elimination or forward selection.

Backward Elimination The backward elimination stepwise method begins by developing an ordinary regression model using all independent variables. All insignificant independent variables

are eliminated in a stepwise fashion. The only independent variables left are the ones that have coefficients that are significantly different from zero. The advantage is that the manager has the opportunity to look at all the independent variables in the model before removing the variables that are not significant.

Forward Selection The forward selection procedure works in the opposite direction of the backward elimination procedure. It begins by selecting a single independent variable that is highly significant—the one highly correlated with the dependent variable. In the next step, a second independent variable is selected based on its ability to explain the remaining unexplained variation in the dependent variable.

The forward selection procedure prevents multicollinearity from occurring. It does this by dropping an insignificant variable that is causing the overlap from the model. The forward selection procedure is widely used in decision-making applications and is generally recognized as a useful regression method. Because the selection process is automatic by the computer, the manager needs to use judgment to make sure the regression model is usable and meaningful.

(H) Econometrics The application of statistical methods to economic data is called econometrics. Econometrics analyzes the relationships between economic variables. It uses multiple regression analysis.

Example

Recent events caused the time series used by an electric utility company to become too unpredictable for practical use. An econometric model is developed to predict the demand for electricity based on factors such as class of service, population growth, and unemployment in the area of service. Since there are three independent variables, multiple regression is used.

(iii) Sensitivity Analysis

Sensitivity analysis is an evaluation of how certain changes in inputs results in what changes in outputs of a model or system (see Exhibit 5.10).

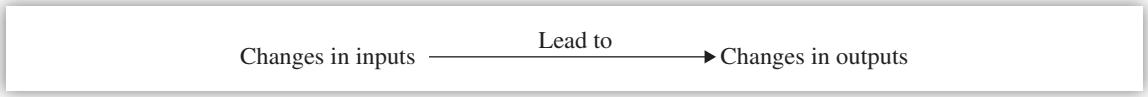


EXHIBIT 5.10 Scope of Sensitivity Analysis

The primary reason that sensitivity analysis is important to managers is that real-world problems exist in a dynamic environment. Change is inevitable. Prices of raw materials change as demand fluctuates, changes in the labor market cause changes in production costs. Sensitivity analysis provides manager with the information needed to respond to such changes without rebuilding the model. For example, bank management can use the sensitivity analysis technique to determine the effects of policy changes on the optimal mix for its portfolio of earning assets.

Computer simulation techniques can be used to perform sensitivity analysis. The capability to ask what-if questions is one of the biggest advantages of computer simulation. The next sections present sensitivity analysis for manufacturing applications, linear programming applications, financial applications, network applications, and inventory applications.

(A) Manufacturing Applications The linking of production process improvement to financial results is critical to a successful computer-integrated manufacturing implementation. Management has established priorities to decrease process variability, shorten feedback time, and reduce support functions. A process model was developed with these parameters: facilities and equipment cost, theoretical materials consumption, actual materials consumption, and supplies cost. Sensitivity analysis was used to study the behavior of those parameters.

Sensitivity analysis was applied to the process model to compare the cash flows associated with various plan alternatives. Testing the model for changes in several parameters indicated that the model is sensitive to process inefficiency, product yields, volume variation, and price variations. Conversely, the model is relatively insensitive to change in labor costs.

The relationships between increased labor efficiency and gross profit can be studied using sensitivity analysis in a manufacturing plant environment.

(B) Linear Programming Applications Sensitivity analysis is the study of how changes in the coefficient of a linear program affect the optimal solution. The optimal solution is a feasible solution that maximizes or minimizes the value of the objective function. The objective function is used to measure the profit or cost of a particular solution.

Sensitivity analysis associated with the optimal solution provides valuable supplementary information for the decision maker. In the linear programming case, sensitivity analysis can be used to answer questions such as

- How will a change in a coefficient of the objective function affect the optimal solution?
- How will a change in the right-hand side value for a constraint affect the optimal solution?

However, there is one prerequisite prior to making the above changes: The optimal solution to the original linear programming problem needs to be in place. The changes are applied to the optimal solution. For this reason, sensitivity analysis is often called postoptimality analysis. For example, in a production environment, sensitivity analysis can help determine how much each additional labor hour is worth and how many hours can be added before diminishing returns set in.

(C) Financial Applications Integer linear programming techniques have been successfully used to solve capital budgeting problems. Only the integer variables are permitted to ensure the values of 0 or 1. They could be of either the all-integer or the mixed-integer type. Fractional values of the decision variable are not allowed. The firm's goal is to select the most profitable projects and budgets for the capital expenditures. The outcome is usually whether the project is accepted (a value of 1) or rejected (a value of 0).

Another advantage of using an integer linear programming technique in a capital budgeting is its ability to handle multiple-choice constraints, such as multiple projects under consideration and only one project can be selected in the end.

Sensitivity analysis is more critical for integer linear programming problems than that for linear programming problems because a small change in one of the coefficients in the constraints can cause a large change in the value of the optimal solution. An example would be that one additional dollar in the budget can lead to a $20 increase in the return.

(D) Network Applications Sensitivity analysis can be performed on the network. It provides the ability to check the feasibility of current schedules and to permit management to experiment with or evaluate the effects of proposed changes.

(E) Inventory Applications It is good to know how much the recommended order quantity would change if the estimated ordering and holding costs had been different. Depending on whether the total annual cost increased, decreased, or remained the same, we can tell whether the economic order quantity (EOQ) model is sensitive or insensitive to variations in the cost estimates.

(iv) Simulation Models

The primary objective of simulation models is to describe the behavior of a real system. A model is designed and developed, and a study is conducted to understand the behavior of the simulation model. The characteristics that are learned from the model are then used to make inferences about the real system. Later, the model is modified (asking what-if questions) to improve the system's performance. The behavior of the model in response to the what-if questions is studied to determine how well the real system will respond to the proposed modifications. Thus, the simulation model will help the decision maker by predicting what can be expected in practice. A key requisite is that the logic of the model should be as close to the actual operations as possible. In most cases, a computer is used for simulation models.

Computer simulation should not be viewed as an optimization technique but as a way to improve the behavior or performance of the system. Model parameters are adjusted to improve the performance of the system. When good parameter settings have been found for the model, these settings can be used to improve the performance of the real system.

The steps involved in a computer simulation model are listed next.

1. A computer simulation model that behaves like or simulates the real-world system is developed.
2. A series of computer runs or experiments is performed to learn about the behavior of the simulation model.
3. The model design is changed to determine if the modifications improve the system performance. What-if questions are asked of the model in this step. Thus, the simulation model helps the manager in predicting the future.

Usually, a simulation exercise is conducted on a computer using a computer simulator. The simulator run by the computer program performs mathematical calculations and keeps track of the simulation results. Examples of calculations in a retail store environment include:

- Number of customers serviced at a retail store during the 20 hours of simulated operations.
- The average profit per hour per store.
- Number of lost customers at a store per hour.
- Average dollar loss per hour per store due to lost customers.

Generic computer programming languages, such as BASIC, FORTRAN, and PASCAL, can be used to develop computer simulators. More specific simulation languages, such as SIMSCRIPT

and GPSS, are favored due to their power. They need few programming statements compared to many statements needed for generic languages.

(A) Simulation Applications in Forecasting Some simulation applications in forecasting are listed next.

- To perform a role-play in order to reflect reality in a person being trained
- To study the performance of a waiting line system
- To simulate traffic flow through a busy street intersection to determine the number of traffic signals required to improve traffic flow
- To simulate airplane flight conditions for training pilots
- To simulate the behavior of an inventory system in order to determine the best order quantity and reorder point
- To model a dry-run evacuation in an office due to fire in a high-risk building
- To create mock disasters to provide experience in dealing with crisis situations, such as product tampering, power outages, and flood
- To train auditors by providing financial statements and operating data to conduct a financial audit or an operational audit, respectively

(B) Simulation Procedures and Approaches Computer simulation is performed using the two basic procedures—heuristic and probabilistic—as shown in Exhibit 5.11.

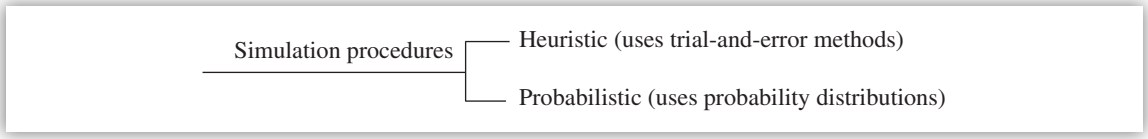


EXHIBIT 5.11 Simulation Procedures

Heuristic procedures do not require probabilistic components. A variety of deterministic values are generated for the decision variables, and the best of the feasible solutions is selected.

When **probabilistic distributions** are involved, it is called the Monte Carlo simulation. Model inputs, such as the number of customer arrivals in a service center, are generated from probability distributions. These models are based on probabilities and time intervals of outcomes. When probabilities are involved, it is called a stochastic model.

Two approaches exist to the logic and record keeping of a simulation model: fixed time period and next event. In the fixed-time-period approach, each time period is of equal length, and the state of the system is updated at either the beginning or the end of each time period. The time between system updates is fixed.

In the next event approach, the time between arrivals and the time to complete service is randomly generated for a customer. The state of the system is updated each time a customer either arrives or completes service. The time between system updates is variable. Exhibit 5.12 presents advantages and disadvantages of simulation models.

Advantages of simulation models	Disadvantages of simulation models
The model solves complex problems where analytical procedures cannot be used.	There is a high cost of model development for design and programming.
The model provides a convenient experimental laboratory. What-if questions can be asked of the model.	The model does not guarantee an optimal solution to a problem. Decision variables are selected that have a good chance of being near the optimal solution. Also, not all values of the decision variables are tried in the model because it is costly to do so.
The danger of obtaining bad solutions to a problem is slight, and the consequences have no effect on the organization.	Simulation may not be able to replicate all situations or complexities that may arise in a real-world case.
The model can be run long enough to reach a steady state that will enable the manager to identify the apparent best decisions.	Participants may tend to generalize from the model. Doing so can create a false sense of confidence concerning their ability to cope with reality.
Learning is active for participants.	
Mistakes are made in a risk-free environment.	
Time spans can be compressed for key problems.	
The model provides immediate feedback concerning proper and improper actions or decisions. Corrective action is timely.	

EXHIBIT 5.12 Advantages and Disadvantages of Simulation Models

ANALYTICAL PROCEDURES VERSUS COMPUTER SIMULATION

- Analytical procedures are best used to solve simple problems.
- Computer simulation is best used to solve complex problems.

The sequence of model activities is

$$\text{Model validation} \rightarrow \text{Model implementation}$$

Model validation is a step in the simulation procedure.

(C) Simulation Model Validation Validation involves verifying that the simulation model accurately describes the real-world system it is designed to simulate. The purpose of model validation is to make sure that it is a reasonable reflection of the real world. The following methods will help to validate the model:

- The simulation results can be compared with the current and past behavior of the real system. The model is run with an actual set of past observations, and the output is compared directly with the behavior of the actual system.
- The model is reviewed by experts who evaluate the reasonableness of the simulation model and the simulation results.
- The assumptions made during model construction need to be revisited, clarified, expanded, and adjusted as needed.

- The model is peer reviewed or desk-checked by programming staff to detect errors. *Improper programming of the model can lead to inaccurate results.*
- The simulated distributions for the probabilistic components can be compared with the corresponding probability distributions in the real system.
- It is good to collect the data on the system after it has reached a stable or steady-state condition. Management is interested in what happens during "normal" business hours of operation. The steady-state condition of the model is synonymous with the normal hours of operation.

(D) Simulation Model Implementation Model implementation includes steps such as searching for: errors, exceptions, gaps between actual and expected, for overlaps or duplications between procedures, and root causes of poor implementation.

(h) Quality Management

Total quality management (TQM) is a strategic, integrated management system for achieving customer satisfaction.[5] It involves all managers and employees and uses quantitative methods to improve an organization's processes continuously. It is not an efficiency (cost-cutting) program, a morale-boosting scheme, or a project that can be delegated to operational managers or staff specialists. Paying lip service to quality improvement by merely using quality slogans to exhort workers is equally disastrous.

KEY CONCEPTS TO REMEMBER: Lessons Learned from TQM

- Learn quality concepts first and tailor them to fit your organization.
- The commitment to change must come from the top management.
- Begin TQM with managers and supervisors who are models and trend setters.
- Data are crucial. Do not guess at what the symptoms or problems are; go out and look at the facts and let them guide the improvement process.
- Recognition of the team members creates enthusiasm.
- TQM is a management system; hence, it cannot be delegated to a quality control department.
- Quality is profit, not cost.
- TQM will reduce costs and risks, increase productivity, and enhance customer satisfaction.

In the TQM context, the standard for determining quality is meeting customer requirements and expectations the first time and every time. Customers have many potential requirements and expectations, depending on the particular product or service and customer needs. Rather than an organization attempting to specify what it views as quality, a TQM approach to quality systematically asks its customers what they want and strives to meet, and even exceed, those requirements. Such an approach helps to identify the elements of quality that are of paramount importance to customers. It also recognizes that customers' expectations may change over time. TQM can be applied equally to manufacturing and service organizations.

[5] U.S. Office of Personnel Management, *Introduction to Total Quality Management* (Washington, D.C.: Author, 1991).

(i) Elements of TQM

The three essential requirements or principles of TQM are: (1) the pursuit of complete customer satisfaction by (2) continuously improving products and services, through (3) the full and active involvement of the entire workforce.

These three principles are met by integrating seven key operating practices.

1. Demonstrating personal leadership of TQM by senior management
2. Strategically planning the short- and long-term implementation of TQM throughout the organization
3. Ensuring that everyone focuses on customers' needs and expectations
4. Developing clearly defined measures for tracking progress and identifying improvement opportunities
5. Providing adequate resources for training and recognition to enable workers to carry the mission forward and reinforce positive behavior
6. Empowering workers to make decisions and fostering teamwork
7. Developing systems to ensure that quality is built in at the beginning and throughout operations

(ii) Strategy of TQM

TQM is an umbrella term and concept that focuses on doing things right in the first place, whether in producing goods or providing services. TQM encompasses the entire organization, both internally from higher-lever employees to lower-level employees and externally from suppliers to customers. A TQM strategy or program includes several elements such as quality concepts and tools, continuous improvement (kaizen), plan-do-check-act (PDCA), just in time (JIT), stakeholder empowerment, benchmarking, International Organization for Standardization (known as ISO), Six Sigma, statistical process control (SPC), and Taguchi's quality loss function. Contrary to popular belief, quality decreases costs and increases profits.

WHAT ARE EXAMPLES OF QUALITY DRIVERS?

- Customers
- Suppliers/vendors
- Employees
- Products
- Services
- Organizational culture
- Organizational policies, procedures, and standards
- Total organizational focus
- Management commitment

(iii) Various Definitions of Quality

Quality has many definitions because it is viewed differently from many perspectives.

The term **judgment-based criteria** is synonymous with superiority or excellence, which is abstract and subjective and difficult to quantify.

Product-based criteria assume that higher levels or amounts of product characteristics are equivalent to higher quality and that quality has a direct relationship with the price.

User-based criteria define that quality is fitness for intended use or how well a product performs its intended function. It is basically dictated by user wants and needs.

Value-based criteria focus on the relationship of usefulness or satisfaction of a product or service to price. This means a customer can purchase a generic product at a lower price if it performs the same way as the brand-name product.

The term **manufacturing-based criteria** refers to conformance to specifications (e.g., engineering or manufacturing) that are important to customers. Taguchi opposes the manufacturing-based definition of quality due to built-in defects to be produced at a higher cost.

The term **customer-driven quality** refers to meeting or exceeding customer expectations. This definition is simple and powerful; hence most companies use it.

WHAT IS THE DIFFERENCE BETWEEN BIG Q AND LITTLE q?

- **Big Q** and **little q** are two contrasting terms in quality.
- **Big Q** focuses on all business products and processes in the entire company.
- **Little q** focuses on all or parts of products and processes in one factory or plant.

A Japanese professor, Noriaki Kano, suggested three classes of customer requirements in understanding the customer's needs in the marketplace. These include dissatisfiers, satisfiers, and delighters. Customers are **dissatisfied** when the features that they assumed or expected are not present in a product. Customers are **satisfied** when the features that they wanted are present in a product. Customers are **delighted** when the features that they did not assume or expect are present in a product because the features exceed their expectations.

Critical to quality (CTQ) is a quality measurement technique that dictates a product's output specifications in terms of a customer's needs, wants, and expectations, whether the customer is internal or external to an organization. CTQ focuses on customer requirements, design and test parameters, mistake proofing, quality robustness, and control charts.

(iv) Return on Quality

Return on quality (ROQ) is similar to ROI in terms of measurement, requiring same attention as ROI.

Quality improvement initiatives have a direct financial impact that cannot be ignored.

ROQ is similar to cost of quality (COQ) in terms of measurement except that COQ takes an internal perspective, such as costs and defects, and ROQ takes an external perspective, such as revenues and customer satisfaction.

COMPARING COQ, ROQ, AND CTQ

COQ takes an internal perspective.

ROQ takes an external perspective.

CTQ takes both internal and external customer perspectives.

ROQ measures expected revenue gains against expected costs associated with quality improvement initiatives.

ROQ is computed as net present value (NPV) of benefits resulting from quality improvement initiatives divided by NPV of costs associated with quality improvement initiatives minus 1.0.

ROQ expressed as a percentage, is computed as follows:

$$\text{ROQ} = [(\text{NPV of Quality benefits})/(\text{NPV of Quality costs})] - 1.00$$

The result is multiplied by 100 to get the percentage.

All benefits and costs are multiplied with the corresponding present value factors to result in NPV of benefits and costs respectively.

(v) What Is Different about TQM?

Although the adoption and integration of the seven operating practices are essential, leaders beginning a TQM effort should bear in mind that realizing the full potential of TQM requires a fundamental cultural change. When this transformation has occurred, everyone in the organization is continuously and systematically working to improve the quality of goods and services, and the processes for delivering them, in order to maximize customer satisfaction. TQM has become a way of managing that is embedded in the culture and environment of the organization, not simply a set of specific management techniques and tools. TQM emphasizes doing each job right the first time.

COMPONENTS OF TQM

- Process management
- Quality teams
- Quality councils
- Ongoing training

It follows that a successful approach to quality improvement requires a long-term commitment and recognition that the effort is an unending journey. Although some early successes can be achieved, a cultural transformation to full use of the TQM approach will occur only gradually.

(vi) Common Areas of Agreement on Quality

Although each of the quality experts (i.e., Deming, Juran, and Crosby — discussed in detail later in this section) has developed his individual approach to quality improvement, the following are some significant common areas of agreement:

- Producing a quality product costs less because there is less waste.
- Preventing quality problems is better than detecting and correcting them.
- Statistical data should be used to measure quality.
- Managers need to take a leadership role in improving quality.
- Managers and employees need training in quality improvement.
- Companies need to develop a quality management system.

A TQM approach to management represents a unique blending of:

- The objective, practical, and quantitative aspects of management (e.g., focus on processes and reliance on quantitative data and statistical analysis for decision making)
- The "soft" aspects of management (e.g., providing a visionary leadership role, promoting a spirit of cooperation and teamwork, and practicing participative management)

Many organizations, when deciding to undertake a TQM effort, focus on one or the other of these general approaches. A fully successful effort requires balanced attention to both.

These areas need to be improved:

- Many managers encourage employee involvement and empowerment, but few organizations adopt the specific practices that bring them about, such as reliance on teams of employees to identify and resolve specific operating problems. Where teams are used, few have been delegated sufficient authority to make changes or have been trained to use the full array of TQM tools.

KEY CONCEPTS TO REMEMBER: Pitfalls to Avoid when Implementing TQM

- Overemphasizing the technical tools at the expense of leadership and management issues
- Applying the tools before the needs are determined
- Rushing the quality improvement process
- Viewing TQM as a budget-cutting tool or employee productivity program
- Conducting mass training before support systems for TQM have been set up

- Although many organizations recognize the importance of measurement and analysis to decision making, many measure the wrong things. Also, few organizations focus on internal processes across functions in order to ensure that quality is built into the production and service system on a continuing basis.
- Many organizations have in place a system they call quality assurance, but these systems are often designed to check for adherence to quality standards at the end of the production process. TQM creates procedures for ensuring quality *throughout* the production and service process.

- Many organizations claim to serve the customer first, but few systematically and rigorously identify the needs of customers, both internal and external, and monitor the extent to which those needs are being met.

(vii) Characteristics of a Quality Organization

When organizations adopt TQM principles and practices, the results have been startling. Workers at all levels focus on their customers' needs and become committed and involved in the quest for quality. Management and workers form a team in seeking continuous improvement. The cumulative result of these changes frequently is a profound change in the overall culture and atmosphere of the organization. Organizations become more streamlined, a larger percentage of workers are involved in line operations, and there is a greater spirit of cooperation and working toward common goals. Perhaps most significantly, a spirit of energy and excitement, even fun, permeates the organization.

Some specific contrasting characteristics that frequently result between the traditional approach and the TQM approach to managing are summarized in Exhibit 5.13.

Traditional approach to managing	TQM approach to managing
The organization structure is hierarchical and has rigid lines of authority and responsibility.	The organization structure becomes flatter, more flexible, and less hierarchical.
Focus is on maintaining the status quo (don't fix it if it ain't broke).	Focus shifts to continuous improvement in systems and processes (continue to improve it even if it ain't broke).
Workers perceive supervisors as bosses or cops.	Workers perceive supervisors as coaches and facilitators. The manager is seen as a leader.
Supervisor/subordinate relationships are characterized by dependency, fear, and control.	Supervisor/subordinate relationships shift to interdependency, trust, and mutual commitment.
The focus of employee efforts is on individual effort; workers view themselves as competitors.	The focus of employee effort shifts to team effort; workers see themselves as teammates.
Management perceives labor and training as costs.	Management perceives labor as an asset and training as an investment.
Management determines what quality is and whether it is being provided.	The organization asks customers to define quality, and develops measures to determine if customers' requirements are met.
Primary basis for decisions is on gut feeling or instinct.	The primary basis for decisions shifts to facts and systems.

EXHIBIT 5.13 Comparison of Traditional Approach to Managing with TQM Approach to Managing

(viii) Quality Assurance, Quality Control, Quality Audit, Quality Circles, and Quality Councils

In order to meet customer quality requirements, the work processes used to produce their products and services must be designed to prevent problems and errors from occurring in the first place.

Quality assurance focuses on the front end of processes, beginning with inputs, rather than the traditional controlling mode of inspecting and checking products at the end of operations, after errors are made. Processes are designed both to prevent errors and to detect and correct them as they occur. As part of the emphasis on prevention and early detection, employees are trained to analyze incoming supplies. Suppliers are asked to assure, assess, and improve their processes and

products or services. The organization establishes a partnership with suppliers and customers to ensure continuous improvement in the quality of the end products and services.

Quality control is an evaluation to indicate needed corrective action, the act of guiding, or the state of a process in which the variability is attributable to a constant system of chance causes. Quality control includes the operational techniques and activities used to fulfill requirements for quality. Often the terms "quality assurance" and "quality control" are used interchangeably, referring to the actions performed to ensure the quality of a product, service, or process.

QUALITY ASSURANCE VERSUS QUALITY CONTROL

- Quality assurance focuses on the front end of processes.
- Quality control focuses on the middle and back end of processes.
- Quality assurance is a management issue.
- Quality control is a technical issue.

Quality audit is a systematic, independent examination and review to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve the objectives.

Quality circles refer to a team of employees (6 to 12) voluntarily getting together periodically to discuss quality-related problems and issues and to devise strategies and plans to take corrective actions. Participative management places a premium on teamwork as the way to solve problems and initiate process improvements, especially issues with cross-functional implications. The focus is on teamwork and processes rather than on individual efforts and tasks. Quality circles should be introduced in an evolutionary manner so that employees feel that they can tap their creative potential.

Establishment of a **quality council** is a prerequisite for implementing a TQM program in the organization. The quality council is similar to an executive steering committee. By establishing a quality council, senior management provides an identity, structure, and legitimacy to the quality improvement effort. It is the first concrete indication that senior management has recognized the need to improve and has begun to change the way the organization conducts its business. The direction that this change will take becomes clear when the quality council publishes its vision, guiding principles, and mission statement. Management needs to support and promote the TQM program, not just sponsor it.

(ix) Concurrent Engineering

Long lead times for introducing new products have been a major problem for many manufacturers. This slowness in introducing new products clears the way for competitive products entering the market.

The focus of concurrent engineering is to reduce the overall product cycle time, which is measured as the elapsed time between research, development, and marketing of a new product. This is called time to market a new product, which is aimed at increasing performance and productivity.

"Concurrent engineering" is defined as a systematic approach to the integrated and overlapping design of products and their related processes, including design, manufacturing, and support.

It requires that, from the beginning, all elements of the product life cycle be evaluated across all design factors to include user requirements, quality cost, and schedule.

The foundation of concurrent engineering is that some 80% to 85% of a product's cost is determined at concept development. Additionally, the integration of support processes early on cuts manufacturing costs while raising quality and reducing development time.

The significant benefits to be obtained from concurrent engineering include:

- Improved quality of design, leading to a reduction in change orders.
- Reduction in product cycle time as a result of using concurrent design rather than sequential design.
- Reduction in manufacturing costs as a result of using multifunction teams to integrate product and process.
- Reduction in scrap and rework as a result of product and process design optimization.

Involving suppliers in product design is also a strategic move for a successful concurrent engineering practice. Concurrent design, a part of concurrent engineering, makes the design relatively fixed, requiring limited engineering change orders, so that little line disruption results. This enables new versions of popular products to be introduced with great speed and ease.

(x) Cost of Quality

The COQ measurement identifies areas for process improvement. The focus of this measurement is to express quality in terms of quantitative and financial language—that is, costs, ROI, cost of poor quality, cost of rework, and so on.

The COQ definition includes the three items:

1. COQ is the cost of making a product conform to quality standards (i.e., quality goods).
2. COQ is the cost of not conforming to quality standards (i.e., waste, loss).
3. COQ is a combination of item 1 and 2.

$$\text{COQ} = \text{Cost of conformance (A)} + \text{Cost of nonconformance (B)}$$

where (A) = Cost to prevent and detect a failure
(B) = Cost to correct a failure

Costs related to quality are usually separated into at least three areas: prevention costs, appraisal costs, and failure costs (see Exhibit 5.14).

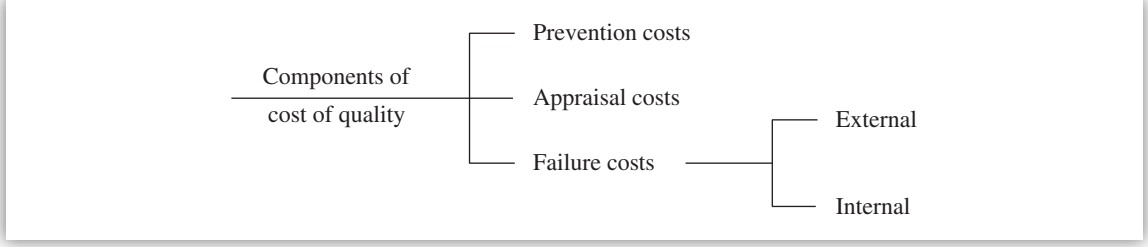


EXHIBIT 5.14 Components of Cost of Quality

(A) Prevention Costs Prevention costs are associated with all the activities that focus on preventing defects. They are the costs of conformance to quality standards. Some major cost categories included in this cost classification are listed next.

- Operator inspection costs
- Supplier ratings
- Supplier reviews
- Purchase-order technical data reviews
- Training
- Supplier certification
- Design reviews
- Pilot projects
- Prototype tests
- Vendor surveys
- Quality design
- Quality department review costs

KEY CONCEPTS TO REMEMBER: Basic Interrelationships among Quality Costs

Money invested in prevention and appraisal can substantially reduce failure costs. In addition to reducing expenses, the reduction in external failure costs results in fewer customer complaints. A dollar invested in a prevention program saves money many times in failure costs.

(B) Appraisal Costs Appraisal costs are associated with measuring, evaluating, or auditing products to ensure conformance with quality standards and performance requirements. Some major cost categories included in this cost classification are listed next.

- Purchasing appraisal costs
- Specifications of supplier product
- Equipment calibration
- Receiving and shipping inspection costs
- Tests
- Product quality audits

(C) Failure Costs Failure costs are associated with evaluating and either correcting or replacing defective products, components, or materials that do not meet quality standards. Failure costs can be either internal failure costs that occur prior to the completion or shipment of a product or the rendering of a service, or external failure costs that occur after a product is shipped or a service is rendered. Examples of internal failure costs include repair, redesign, reinspection, rework, retesting, sorting, and scrap. Examples of external failure costs include product warranty charges, returns, and recalls; liability suits; and field service staff training costs.

Quality metrics can be developed for the cost of quality measurement to help managers monitor quality. These metrics include:

- Total cost of quality as percentage of revenue by year.
- Cost of conformance as percentage of total cost of quality.
- Cost of nonconformance as percentage of total cost of quality.

(xi) Quality Tools

Either an auditor or an auditee can use quality tools. These tools can be used to analyze processes, prioritize problems, report the results, and evaluate the results of a corrective action plan. The seven quality control tools are listed next.

1. Check sheets
2. Histograms
3. Scatter diagrams
4. Pareto diagrams
5. Flowcharts
6. Cause-and-effect diagrams
7. Control charts

Later, seven other tools became popular. These are called the seven quality management tools. These management tools include:

1. Affinity diagrams (also called the KJ method)
2. Tree diagrams
3. Process decision program charts(PDPCs)
4. Matrix diagrams
5. Interrelationship digraphs
6. Prioritization matrices
7. Activity network diagrams

The seven quality management tools are modern while the seven quality control tools are traditional. Both tools are used as needed.

QUALITY CONTROL TOOLS VERSUS QUALITY MANAGEMENT TOOLS

- The seven quality control tools are used for quantitative data analysis.
- The seven quality management tools are used for qualitative data analysis.

(A) Seven Quality Control Tools The traditional, original seven quality control tools were adequate for data collection and analysis. Each tool is discussed briefly next.

Check Sheets Check sheets are used for collecting data in a logical and systematic manner. The data collected can be used in constructing a quality control chart, Pareto diagram, or histogram. The check sheet enables the user to gather and organize data in a format that permits efficient and easy analysis of data.

Process improvement is facilitated by the determination of what data or information are needed to reduce the difference between customer needs and process performance. Some examples of data that can be collected are listed next.

- Process variables, including size, length, weight, and diameter
- Number of defects generated by each cause
- Product characteristics
- Costs
- Vendors
- Inspection procedures
- Customer profiles
- Employee attitudes
- Defect location

The idea is that once these data are collected and analyzed, the cause can be found and a plan to eliminate the problem can be implemented.

Histograms A histogram is a frequency distribution diagram in which the frequencies of occurrences of the different variables being plotted are represented by bars. The purpose is to determine the shape of the graph relative to the normal distribution (or other distributions). Histograms often are confused with bar graphs, in which the frequency of a variable is indicated by the height of the bars. In a histogram, the frequency is indicated by the *area* of the bar. Histograms can be used only with variable data, which require measurements on a continuous scale. Only one characteristic can be shown per histogram, and at least 30 observations representing homogeneous conditions are needed.

QUALITY CONTROL TOOLS

The seven quality control tools include check sheets, histograms, scatter diagrams, Pareto diagrams, flowcharts, cause-and-effect diagrams, and control charts.

A histogram is a frequency distribution, in which the area of each bar is always proportional to the actual percentage of the total falling in a given range. If the bars are of equal length, then the histogram is equivalent to a bar graph, in which the relative size of the bars depends only on their heights. A histogram can be compared to the normal distribution (or other distribution). For example, if the graph is off center or skewed, this may indicate that a process requires adjustment. Histograms are essentially used for the same applications as bar graphs, except that the horizontal scale in a histogram must be numerical, usually representing a continuous random variable.

A bar graph is a frequency distribution diagram in which each bar represents a characteristic or attribute, and the height of the bar represents the frequency of that characteristic. The horizontal axis may represent a continuous numerical scale (e.g., hours) or a discrete non-numerical scale (e.g., phases of a project). Generally, numerical-scale bar graphs in which the bars have equal widths are more useful for comparison purposes; numerical-scale bar charts with unequal intervals can be misleading because the characteristics with the largest bars (in terms of area) do not necessarily have the highest frequency. Bar graphs are used to compare the frequencies of different attributes (e.g., number or percentage of problem reports by phase).

Scatter Diagrams A scatter diagram is a plot of the values of one variable against those of another variable to determine the relationship between them. These diagrams are used during analysis to understand the cause-and-effect relationship between two variables. Scatter diagrams are also called correlation diagrams.

If the data points fall approximately in a straight line, this indicates that there is a linear relationship, which is positive or negative, depending on whether the slope of the line is positive or negative. Further analysis using the method of least squares can be performed. If the data points form a curve, then there is a nonlinear relationship. If there is no apparent pattern, this may indicate no relationship. However, another sample should be taken before making such a conclusion.

The method of least squares can be used in conjunction with scatter diagrams to obtain a more precise relationship between variables. It is used to determine the equation of the regression line (i.e., the line that "best fits" the data point). With this equation, one can approximate values of one variable when given values of the other.

Pareto Diagrams A Pareto diagram is a special bar graph in which the bars are arranged in descending order of magnitude. The purpose of Pareto analysis, using Pareto diagrams, is to identify the major problems in a product or process or, more generally, to identify the most significant causes for a given effect. This allows a developer to prioritize problems and decide which problem area to work on first.

Pareto analysis is based on the 20/80 rule, which states that approximately 20% of the causes (the "vital few") account for 80% of the effects (problems). The vital few can be determined by drawing a cumulative percentage line and noting which bars are to the left of the point marking 80% of the total count. The vital few are usually indicated by significantly higher bars and/or a relatively steep slope of the cumulative percentage line.

Pareto diagrams (charts) can be helpful in determining whether efforts toward process improvement are producing results. These diagrams are useful when the process is stable; they are not effective if used on a chaotic process because the process is not ready for improvement. The process must first be stabilized through the use of control charts. *Root cause analysis is performed using Pareto diagrams.*

Pareto diagrams can be drawn showing before-and-after improvements, demonstrating the effect of the improvements. Pareto diagrams are powerful tools when used in this way because they can mobilize support for further process improvement and reinforce the continuation of current efforts. Pareto diagrams are usually drawn as pie charts, histograms, or vertical bar charts. Pareto

diagrams focus on the "vital few" instead of the "trivial many." When arranged from greatest to least, the Pareto chart graphically indicates which problems should be handled first.

Flowcharts A flowcharting tool can be used to document every phase of a company's operation, for example, from order taking to shipping in a manufacturing company. It is an effective way to break down a process or pinpoint a problem. Flowcharting can be done at both the summary level and the detailed level, serving different user needs.

Flowcharting is a first step toward the documentation of a process required for ISO 9000 and other quality awards. In this way, problems can be traced quickly to the right source and corrected properly. Also, flowcharts can be used as a training tool or a reference document on the job.

A process map is similar to a flowchart. Mapping is the activity of developing a detailed flowchart of a work process showing its inputs, tasks, and activities in sequence. A process map provides a broader perspective than typical flowcharts.

Cause-and-Effect Diagrams One form of a C&E diagram is used for process analysis. It is used when a series of events or steps in a process creates a problem and it is not clear which event or step is the major cause of the problems. Each process or subprocess is examined for possible causes; after the causes from each step in the process are discovered, significant root causes of the problem are selected, verified, and corrected. C&E diagrams are also called fishbone or Ishikawa diagrams (after their inventor).

C&E diagrams should be used as a framework for collecting efforts. If a process is stable, the diagram will help organize efforts to improve the process. If a process is chaotic, the diagram will help uncover areas that can help stabilize the process.

Control Charts A control chart assesses a process variation. Control charts display sequential process measurements relative to the overall process average and control limits. The upper and lower control limits establish the boundaries of normal variation for the process being measured. Variation within control limits is attributable to random or chance causes, while variation beyond control limits indicates a process change due to causes other than chance—a condition that may require investigation. The upper control limit and lower control limit give the boundaries within which observed fluctuations are typical and acceptable. They are usually set, respectively, at three standard deviations above and below the mean of all observations.

There are many different types of control charts. They include:

- np charts, where "np" is number of nonconforming units.
- p charts, where "p" is fraction of nonconforming units.
- c charts, where "c" is number of nonconformities.
- u charts, where "u" is number of nonconformities per unit.
- X charts, where "X" is a single observed value.
- XB charts, where "XB" is X-Bar
- R charts, where "R" is a range.

- XM charts, where "XM" is a median.
- MR charts, where "MR" is a moving range.

A run chart is a simplified control chart, in which the upper and lower control limits are omitted. The purpose of the run chart is more to determine trends in a process rather than variation in a process. Run charts can be used effectively to monitor a process—for example, to detect sudden changes and to assess the effects of corrective actions. Run charts provide the input for establishing control charts after a process has matured or stabilized in time. Limitations of this technique are that it analyzes only one characteristic over time, and it does not indicate if a single data point is an outlier.

Dr. Genichi Taguchi, a Japanese statistician and Deming Prize winner, developed what is called Taguchi method, the off-line quality control method, which includes product and process design. This is contrasted to on-line quality control in which quality control activities are focused on control charts and process control methods. Taguchi's methods provide a system to develop specifications, design those specifications into a product and/or process, and produce products that continuously surpass said specifications. There are seven aspects to off-line quality control.

1. The quality of a manufactured product is measured by the total loss to society created by that product.
2. Continuous quality improvement and cost reduction are necessary for an organization's health in a competitive economy.
3. Quality improvement requires the never-ending reduction of variation in product and/or process performance around nominal values.
4. Society's loss due to performance variation often is proportional to the square of the deviation of the performance characteristic from its nominal value.
5. Product and process design can have a significant impact on a product's quality and cost.
6. Performance variation can be reduced by exploiting the nonlinear effects between a product's and/or process's parameters and the product's desired performance characteristics.
7. Product and/or process parameter settings that reduce performance variation can be identified with statistically designed experiments.

(B) Seven Quality Management Tools The traditional quality tools were adequate for data collection and analysis, but the seven modern tools allow better identification, planning, and coordination in quality problem solving. These new tools include affinity diagrams (also called KJ method), tree diagrams, PDPC, matrix diagrams, interrelationship digraphs, prioritization matrices, and activity network diagrams. Each tool is discussed briefly.

Affinity Diagrams The affinity diagram is a data reduction tool in that it organizes a large number of qualitative inputs into a smaller number of major categories. These diagrams are useful in analyzing defect data and other quality problems, and used in conjunction with C&E diagrams or interrelationship digraphs.

Tree Diagrams A tree diagram can be used to show the relationships of a production process by breaking it down from a few larger steps into many smaller steps. The greater the detail of

steps, the better simplified they are. Quality improvement actions can start from the rightmost of the tree to the leftmost.

Process Decision Program Charts The PDPC is a preventive control tool in that it prevents problems from occurring in the first place and mitigates the impact of the problems if they do occur. From this aspect, it is a contingency planning tool. The objective of the tool is to determine the impact of the failures or problems on project schedule.

Matrix Diagrams A matrix diagram is developed to analyze the correlations between two groups of ideas with the use of a decision table. This diagram allows one to systematically analyze correlations. Quality function deployment (QFD) is an extension of the matrix diagram. The American Supplier Institute defines QFD as "a system for translating consumer/customer requirements into appropriate company requirements at each stage, from research and product development, to engineering and manufacturing, to marketing/sales and distribution."

The QFD is a structured method and uses a series of charts called quality tables to provide the discipline and communication required to focus on answering three action-oriented questions: What? How? and How much? QFD can be used both for products and services.

Interrelationship Digraphs The interrelationship digraph is used to organize disparate ideas. Arrows are drawn between related ideas. An idea that has arrows leaving it but none entering is a root idea. More attention is given to the root ideas for system improvement. The digraph is often used in conjunction with affinity diagrams.

Prioritization Matrices Prioritization matrices are used to help decision makers determine the order of importance of the activities being considered in a decision. Key issues and choices are identified for further improvement. These matrices combine tree diagrams and matrix diagrams.

QUALITY MANAGEMENT TOOLS

The seven quality management tools include affinity diagram (also called KJ method), tree diagram, PDPC, matrix diagram, interrelationship digraph, prioritization matrices, and activity network diagram.

Activity Network Diagrams Activity network diagrams are project management tools to determine which activities must be performed, when they must be performed, and in what sequence. These diagrams are similar to program evaluation and review techniques (PERT) and the critical path method (CPM), two popular tools in project management. Unlike PERT and CPM, activity network diagrams are simple to construct and require less training to use.

(C) Plan-Do-Check-Act Cycle The PDCA cycle was first known as the Shewhart cycle and later known as the Deming cycle. It is a core management tool for problem solving and quality improvement. The PDCA cycle can be used for planning and implementing quality improvements. The "plan" calls for developing an implementation plan for initial effort followed by organization-wide effort.

The "do" part carries out the plan on a small scale using a pilot organization, and later on a large scale. The "check" phase evaluates lessons learned by pilot organization. The "act" phase uses lessons learned to improve the implementation. It supports both old and new quality tools.

(D) Stratification Stratification is a procedure used to describe the systematic subdivision of population or process data to obtain a detailed understanding of the structure of the population or process. It is not to be confused with a stratified sampling method. Stratification can be used to break down a problem to discover its root causes and can establish appropriate corrective actions, called countermeasures.

Stratification is important to the proper functioning of the Deming PDCA cycle. *Failure to perform meaningful stratification can result in the establishment of inappropriate countermeasures, which can then result in process or product deterioration in quality.*

STRATIFICATION VERSUS PARETO DIAGRAM VERSUS C&E DIAGRAM

- Stratification can be used when performing root cause analysis with Pareto diagrams. A problem can be broken down into subcomponents, and each subcomponent can be further broken down into its subcomponents, and so on. Then attention should be paid to one or more of the root causes of a process or product problem, from which countermeasures can be established to resolve the problem.
- Stratification can also be used when performing root cause analysis with C&E diagrams. A C&E diagram can be used to stratify one bar from a Pareto diagram at a time to get an in-depth understanding of the corresponding cause (bar) before any other cause (bar) is studied.

(xii) Quality Models and Awards

A system should be put in place to allow the organization to determine systematically the degree to which product and services please customers and to focus on internal process improvement. Data should be collected on features of customer satisfaction such as responsiveness, reliability, accuracy, and ease of access. The measurement systems should also focus on internal processes, especially on processes that generate variation in quality and cycle time. *Cycle time is the time required from conception to completion of an idea or a process.* When customer data indicates a problem, or when the organization wants to raise the level of customer satisfaction, the organization should focus on improving the processes that deliver the product or service.

In order to ensure that processes are continuously improved, data should be collected and analyzed on a continuing basis, with particular attention to variation in processes. The causes of variation are examined to determine whether they result from special circumstances (special causes) or from recurring ("common") causes. Different strategies should be adopted to correct each occurrence. The immediate objectives of the analysis and measurement effort are to reduce rework, waste, and cycle time and to improve cost effectiveness and accuracy. The ultimate objectives are to ensure that the organization understands the extent to which customer satisfaction is being realized, where there are deficiencies, and why, and to isolate causes that can be attacked systematically.

(A) Three Quality Preachers We will discuss quality models from the viewpoints of three quality preachers: (1) Deming, (2) Juran, and (3) Crosby.

Deming Quality Model According to Deming, good quality does not necessarily mean high quality. It is, rather, "a predictable degree of uniformity and dependability, at low cost, and suited to the market." Deming recognizes that the quality of any product or service has many scales, and it may get a high mark on one scale and a low mark on another. In other words, quality is whatever the customer needs and wants. Since the customer's requirements and tastes are always changing, the solution to defining quality in terms of the customer is to constantly conduct customer research.

Deming said people are eager to do a good job and are disturbed when they are unable to do so because of limitations imposed by management. Deming's basic philosophy on quality is that productivity improves as variability decreases. Since all things vary, he says, that is why the statistical method of quality control is needed. "Statistical control does not imply absence of defective items. It is a state of random variation, in which the limits of variation are predictable," he explains.

There are two types of variation: chance and assignable. According to Deming: "The difference between these is one of most difficult things to comprehend." It is a waste of time and money to look for the cause of the chance variation, yet, he says, this is exactly what many companies do when they attempt to solve quality problems without using statistical methods. He advocates the use of statistics to measure performance in all areas, not just conformance to product specifications. Furthermore, he says it is not enough to meet specifications; one has to keep working to reduce the variation as well.

Inspection, whether of incoming or outgoing goods, is, according to Deming, too late, ineffective, and costly. "Inspection does not improve quality, nor guarantee it." Moreover, inspection is usually designed to allow a certain number of defects to enter the system. For example, a company that buys items with an acceptable quality level of 3% is, in effect, telling the vendor that it can send three bad items out of every 100. "The vendor will be pleased to meet these requirements," says Deming.

Deming says that judging quality requires knowledge of the "statistical evidence of quality" and that companies dealing with vendors under statistical control can eliminate inspection. "You will note from the control charts that came along with the product, far better than any inspection can tell you, what the distribution of quality is, and what it will be tomorrow." In this way, quality is predictable, and one can also safely predict that the vendor's quality will improve over time. "One of the first steps for managers of purchasing to take is to learn enough about the statistical control of quality to be able to assess the qualifications of a supplier, to be able to talk to him in statistical language," says Deming.

Deming also points out that simply checking the specifications of incoming materials may not be enough if the material encounters problems in production. "Specifications cannot tell you the whole story. The supplier must know what the material is to be used for." Deming is critical of most producers for qualifying vendors on quality because, once qualified, the vendor "has discharged his responsibility, and the purchaser accepts whatever he gets." The only effective way to qualify vendors is to see if their management abides by Deming's 14 points, uses statistical process control, and is willing to cooperate on the tests and use of instruments and gauges.

The best recognition one can give a quality vendor, according to Deming, is to give that vendor more business. He points out that requiring statistical evidence of process control in selecting vendors would mean, in most companies, a drastic reduction in the number of vendors they deal with simply because not that many vendors would qualify. Nevertheless, he says, this is the only way to choose vendors, even if that means relying on a single source for critical items.

In fact, Deming advocates single sourcing. "A second source, for protection, for every item purchased is a costly practice," he says. The advantages of single sourcing include better vendor commitment, eliminating small differences between products from two suppliers, and simplifying accounting and paperwork. A disadvantage is the risk of depending on one supplier without any backup alternatives.

As to the fact that relying on a single source can often mean paying a higher price, Deming says: "The policy of forever trying to drive down the price of anything purchased, with no regard to quality and service, can drive good vendors and good service out of business. The ways of doing business with vendors and customers that were good enough in the past must now be revised to meet new requirements of quality and productivity."

DEMING'S 14 POINTS FOR MANAGEMENT

1. Create constancy of purpose toward improvement of products and services.
2. Adopt the new philosophy. We can no longer live with commonly accepted levels of delays, mistakes, defective materials, and defective workmanship.
3. Cease dependence on mass inspection. Require, instead, statistical evidence that quality is built in.
4. End the practice of awarding business on the basis of price tag.
5. Find problems. It is management's job to work continually on the system.
6. Institute modern methods of training on the job.
7. Institute modern methods of supervision of production workers. The responsibility of foremen must be changed from quantity to quality.
8. Drive out fear, so that everyone may work effectively for the company.
9. Break down barriers between departments.
10. Eliminate numerical goals, posters, and slogans for the workforce, asking for new levels of productivity without providing methods.
11. Eliminate work standards that prescribe numerical quotas.
12. Remove barriers that stand between the hourly worker and his right to pride of workmanship.
13. Institute a vigorous program of education and retraining.
14. Create a structure in top management that will push every day on the preceding 13 points.

Juran Quality Model According to Jospeh M. Juran, there are two kinds of quality: "fitness for use" and "conformance to specifications." To illustrate the difference, he says a dangerous product could meet all specifications but not be fit for use. Juran points out that the technical aspects of quality control had been well covered but that firms did not know how to manage for quality. He identifies some of the problems as organizational, communication, and coordination of functions—in other words, the human element.

Juran talks about three basic steps to progress: (1) structured annual improvements combined with devotion and a sense of urgency, (2) massive training programs, and (3) upper management leadership. In his view, less than 20% of quality problems are due to workers; the remainder is caused by management.

JURAN'S 10 STEPS TO QUALITY IMPROVEMENT

1. Build awareness of the need and opportunity for improvement.
2. Set goals for improvement.
3. Organize to reach the goals (establish a quality council, identify problems, select projects, appoint teams, designate facilitator).
4. Provide training.
5. Carry out projects to solve problems.
6. Report progress.
7. Give recognition.
8. Communicate results.
9. Keep score.
10. Maintain momentum by making annual improvement part of the regular systems and processes of the company.

Crosby Quality Model According to Philip B. Crosby's definition, quality is conformance to requirements, and it can be measured only by the cost of nonconformance. "Don't talk about poor quality or high quality. Talk about conformance and nonconformance," he says. This approach means that the only standard of performance is zero defects. Crosby encourages "prevention (perfection)" as opposed to "inspection," "testing," and "checking."

CROSBY'S 14 STEPS TO QUALITY IMPROVEMENT

1. Make it clear that management is committed to quality.
2. Form quality improvement teams with representatives from each department.
3. Determine where current and potential quality problems lie.
4. Evaluate the cost of quality and explain its use as a management tool.
5. Raise the quality awareness and personal concern of all employees.
6. Take actions to correct problems identified through previous steps.
7. Establish a committee for the zero defects program.
8. Train supervisors to actively carry out their part of the quality improvement program.
9. Hold a zero defects day to let all employees realize that there has been a change.
10. Encourage individuals to establish improvement goals for themselves and their groups.
11. Encourage employees to communicate to management the obstacles they face in attaining their improvement goals.
12. Recognize and appreciate those who participate.
13. Establish quality councils to communicate on a regular basis.
14. Do it all over again to emphasize that the quality improvement program never ends.

(B) Malcolm Baldrige National Quality Award The Malcolm Baldrige National Quality Award is an annual award to recognize U.S. companies that excel in quality management and quality achievement. The award promotes:

- Awareness of quality as an increasingly important element of competitiveness.
- Understanding of the requirements for quality excellence.
- Sharing of information on successful quality strategies and the benefits derived from implementation of these strategies.

Award criteria goals include delivery of ever-improving value to customers and improvement of overall company operational performance. The award criteria are built on a set of core values and concepts. Together, these values and concepts represent the underlying basis for integrating the overall customer and company operational performance requirements. These core values and concepts are listed next.

- Customer-driven quality
- Leadership
- Continuous improvement
- Employee participation and development
- Fast response
- Design quality and prevention
- Long-range outlook
- Management by fact
- Partnership development
- Corporate responsibility and citizenship

The core values and concepts are embodied in seven categories:

1. Leadership
2. Information and analysis
3. Strategic quality planning
4. HR development and management
5. Management of process quality
6. Quality and operational results
7. Customer focus and satisfaction

(C) European Quality Award The European Quality Management Association has set up a European equivalent to the U.S. Baldrige program, the European Quality Award (EQA). The quality measures for EQA are listed next.

- Leadership
- Information and analysis

- Strategic quality planning
- HR development and management
- Management of process quality
- Quality and operational results
- Customer focus and satisfaction
- Financial results
- Environmental concerns

(xiii) Six Sigma

Six Sigma is an approach to measuring and improving product and service quality. In Six Sigma terminology, a defect (nonconformance) is any mistake or error that is passed on to the customer. It redefines quality performance as defects per million opportunities (DPMO), as follows:

$$\text{DPMO} = (\text{Defects per unit}) \times 1{,}000{,}000/\text{Opportunities for error where defects per unit}$$
$$= \text{Number of defects discovered/Number of units produced}$$

Six Sigma represents a quality level of at most 3.4 defects per million opportunities. Its goal is to find and eliminate causes of errors or defects in processes by focusing on characteristics that are critical to customers.

Six Sigma Metrics The recognized benchmark for Six Sigma implementation is GE. GE's Six- Sigma problem-solving approach (DMAIC) employs five phases: (1) define, (2) measure, (3) analyze, (4) improve, and (5) control.

The define (D) phase focuses on identifying customers and their priorities, identifying a project suitable for Six Sigma efforts based on business objectives as well as customer needs and feedback, and identifying critical-to-quality characteristics (CTQs) that the customer considers to have the most impact on quality. Specific tools useful in the define phase include C&E diagram, brainstorming, and process mapping ("as is").

The measure (M) phase focuses on determining how to measure the process and how it is performing and identifying the key internal processes that influence CTQs and measure the defects currently generated relative to those processes. Specific tools useful in the measure phase include systems analysis, C&E diagram, process mapping, and common cause and special cause identification.

The analyze (A) phase focuses on determining the most likely causes of defects and understanding why defects are generated by identifying the key variables that are most likely to create process variation. Specific tools useful in the analyze phase include SPC and process mapping.

The improve (I) phase focuses on identifying means to remove the causes of the defects, confirming the key variables and quantifying their effects on the CTQs, identifying the maximum acceptable ranges of the key variables and a system for measuring deviations of the variables, and modifying the process to stay within the acceptable range. Specific tools useful in the improve phase include brainstorming (idea gathering), process mapping ("should be"), and quality function deployment (house of quality and voice of the customer).

The control (C) phase focuses on determining how to maintain the improvements and putting the tools in place to ensure that the key variables remain within the maximum acceptable ranges under the modified process. Specific tools useful in the control phase include mistake proofing and institutionalization.

The concept behind Six Sigma is similar to TQM, which is the integration of human and process elements of improvement. Human elements include management leadership, a sense of urgency, focus on results and customers, team processes, and culture change. Process elements include the use of process management techniques, analysis of variation and statistical methods, a disciplined problem-solving approach, and management by fact.

According to the American Society for Quality (ASQ), several key principles are necessary for effective implementation of Six Sigma.

- Committed leadership from top management
- Integration with existing initiatives, business strategy, and performance measurement
- Process thinking
- Disciplined customer and market intelligence gathering
- A bottom-line orientation
- Leadership in the trenches

  This includes technical and nontechnical employees and managers. It also includes:

  - Champions, who are fully trained business leaders who promote and lead the deployment of Six Sigma in a significant area of the business
  - Master black belts, who are fully trained quality leaders responsible for Six Sigma strategy, training, mentoring, deployment, and results
  - Black belts, who are fully trained Six Sigma experts who lead improvement teams, work projects across the business, and mentor green belts
  - Green belts, who are full-time teachers with quantitative skills as well as teaching and leadership ability(they are fully trained quality leaders responsible for Six Sigma strategy, training, mentoring, deployment, and results)
  - Team members, who are individuals who support specific projects in their area
- Training
- Continuous reinforcement and rewards

Six Sigma Tools Six Sigma tools can be categorized into eight general groups, which integrate the tools and the methodology into management systems across the organization.

1. Elementary statistical tools include basic statistics, statistical thinking, hypothesis testing, correlation, and simple regression.
2. Advanced statistical tools include design of experiments, analysis of variance, and multiple regression.
3. Product design and reliability tools include quality function deployment (QFD) and failure mode and effects analysis (FMEA).

4. Measurement tools include process capability and measurement systems analysis.
5. Process improvement tools include process improvement planning, process mapping, and mistake proofing (Poka-Yoke).
6. Implementation tools focus on organizational effectiveness and facilitation of meetings and communication.
7. Teamwork tools focus on team development and team assessment.
8. Process control tools include quality control plans and SPC.

Six Sigma Players Several Six Sigma players exist in the planning and implementation of a Six Sigma program in an organization, including white belts (at the bottom), green belts, black belts, master black belts, project champions, and senior champions (at the top) in the Six Sigma hierarchy. All these players assume defined roles and responsibilities and need specific training of varying lengths to make the Six Sigma program a success.

White belts are hourly employees who need basic training in Six Sigma goals, tools, and techniques to help green belts and black belts on their projects.

Green belts are salaried employees who have a dual responsibility in implementing Six Sigma in their function and carrying out their regular duties in that function. They gather and analyze data in support of a black belt project and receive a simplified version of black belt training. Yellow belts are seasoned salaried employees who are familiar with quality improvement processes.

Black belts are salaried employees who have a full-time responsibility in implementing Six Sigma projects. They require hard skills and receive extensive training in statistics and problem-solving and decision-making tools and techniques, as they train green belts. Black belts are very important to Six Sigma's success.

Master black belts are salaried employees who have a full-time responsibility in implementing Six Sigma projects. They require soft skills, need some knowledge in statistics, and need more knowledge in problem-solving and decision-making tools and techniques, as they train black belts and green belts.

Senior champions are sponsors and executives in a specific business function and manage several project champions at the business unit level who, in turn, manage specific projects. Senior champions develop plans, set priorities, allocate resources, and organize projects. Project champions deploy plans, manage projects that cut across the business functions and provide managerial and technical guidance to master black belts and black belts. All champions require soft skills.

WHICH SIX SIGMA PLAYER DOES WHAT?

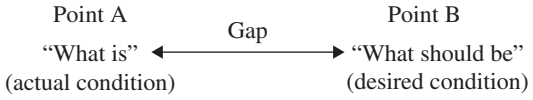
- White belts help green belts and black belts.
- Green belts help black belts.
- Black belts help master black belts.
- Master black belts help project champions.
- Project champions help senior champions.
- Senior champions decide what gets done while project champions, master black belts, and black belts decide how to get it done.

(i) Decision Analysis

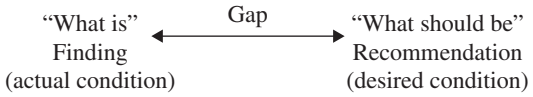
Both problem-solving and decision-making topics with theories, concepts, and tools are described to show how problems can solved with the right kind of decisions.

(i) Problem Solving

(A) What Is a Problem? In this section, we first discuss the theory behind problem solving followed by its application to internal auditing. A problem exists when there is a gap between "what is" and "what should be." Individuals recognize a problem when they feel frustrated, frightened, angry, or anxious about a situation. Organizations recognize problems when: outputs and productivity are low; quality of products and services is poor; people are not cooperating, sharing information, or communicating; or there is a dysfunctional degree of conflict among people in various departments. When the gap between "what is" and "what should be" causes anxiety and inefficiency, something needs to be done to solve the problem.



A problem is the gap between where one is and where one wants to be. The process of closing the gap between the actual situation and the desired situation is problem solving. Problems do not solve themselves—people solve problems. In a way, audit reports are problem-solving tools. The deficiency findings contained in the audit report describe and compare the actual condition (what is) with the desired condition (what should be), thus creating a gap. The auditor's recommendations are aimed at closing this gap. Audit work is then a type of problem solving. According to the IIA Standard 430 — *Communicating Results*, audit findings are the result of comparing "what should be" with "what is" and analyzing the impact. This is shown next.



If internal auditing reports are problem-solving tools, then internal auditors are problem solvers since the audit work is done by auditors, who then prepare the report. The management principle behind the problem solving is Theory Y in that both managers and auditors will take responsibility for and are interested in solving organizational problems. Effective written and oral communication skills are prerequisites to effective problem-solving skills.

(B) Problem-Solving Process Problem solving is a systematic process of bringing the actual situation or condition closer to the desired condition. Although there are many ways to handle problems, Robert Kreitner defines managerial problem solving as a four-step sequence: (1) identifying the problem, (2) generating alternative solutions, (3) selecting a solution, and (4) implementing and evaluating the solution.[6] These four steps are depicted in Exhibit 5.15 with a possible recycling from Steps 3 and 4 to Steps 1 and 2.

[6] Robert Kreitner, *Management*, 9th ed. (Boston: Houghton Mifflin, 2004).

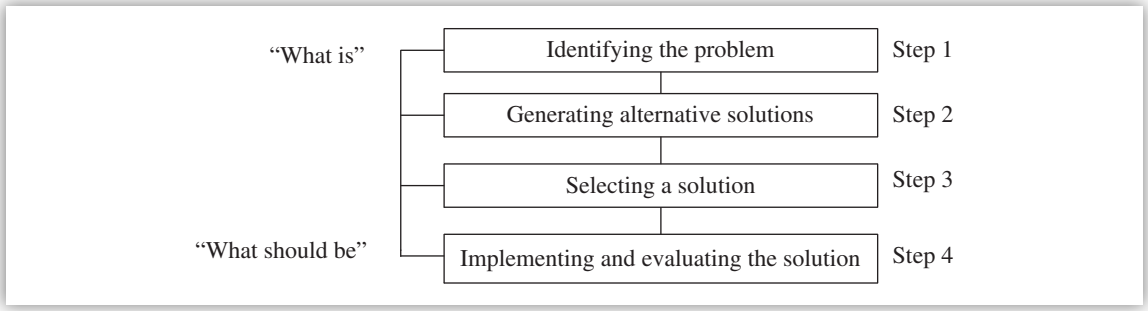


EXHIBIT 5.15 Steps in the Problem-Solving Process

Step 1: Identifying the Problem The scope of this step includes awareness of a problem, problem diagnosis and identification, and criteria for solution. Identifying the problem is a major, crucial work. It can consist of initial awareness that something is not right. The problem-solving cycle begins with some identified need. If there is no need, the cycle is unnecessary. Some examples of problem indications are listed next.

- A production manager finds a gap between actual weekly production and the desired level.
- A plant department manager finds a gap between actual attendance levels and desired attendance levels.
- A marketing manager finds a gap between the actual market share for a product and the desired market share.
- A financial manager finds a gap between the actual earnings for a quarter and the desired earnings.
- An audit manager finds a gap between the actual report issuance time and the desired report issuance time.

The adage "A fully developed problem is half solved" is truly applicable here. Problem identification is a two-dimensional process. The first dimension deals with the degree or condition of the problem, and the second one addresses the structure of the problem. Each dimension is discussed briefly.

Degree or Condition of the Problem

It is necessary to understand the degree or intensity of a problem in order to plan the appropriate timing and strategies for its solutions. There are three issues involved here: stable, dynamic, and critical.

A **stable issue** is one in which there is a little or no controversy. The decision maker requires little input and can usually solve the problem in a task-oriented fashion. A **dynamic issue** is one around which there is a good deal of controversy and the decision maker turns to a group for input. Leadership is process-oriented. A **critical issue** is immersed in controversy and requires resolution by senior management. Leadership is most effective in resolving critical issues when it is task as well as process oriented.

Structure of the Problem

Structure has to do with the routineness of the decision required. Questions to ask include: How much is known or understood about the problem? Is this a new problem? Do mechanisms exist within the organization to deal with this problem?

Two types of problems exist: structured and unstructured problems. Structured problems have only one unknown and have routine programs available to respond; unstructured problems have at least two unknowns and no routine programs available to respond. As an organization faces the same unstructured problem repeatedly, it gradually develops mechanisms to respond to the problem, which then becomes structured.

After being aware of the problem, it is good to obtain valid information about the problem in order to identify what it is. Problem identification is a description of the present conditions, the symptoms, and the underlying causes. The outcome should be a written statement identifying the root problem.

Defining the criteria for solution addresses what the desired condition should be. This condition should be measurable and specific. True agreement on the criteria that a solution must meet is important to help avoid conflict at a later time in the problem-solving cycle.

STUMBLING BLOCKS FOR PROBLEM FINDERS

- *Defining the problem according to a possible solution* means ruling out alternative solutions in the way one states a problem
- *Focusing on narrow, low-priority areas* means ignoring organization goals and objectives
- *Diagnosing problems in terms of their symptoms* means inability to differentiate between short-run and long-run handling of symptoms. Treating symptoms rather than underlying causes is acceptable in the short run but is not acceptable in the long run since symptoms tend to reappear. The real cause(s) of the problem should be discovered. Causes are variables, whether they are controllable or uncontrollable. The problem can be solved or the gap can disappear by focusing on adding or removing these variables.

Step 2: Generating Alternative Solutions During this step, the problem solver needs to identify the possible methods and means to get from what is to what should be. The information collection effort includes researching new ideas and methods and resources for achieving the goals. Generating alternative solutions is time consuming and demanding mental work.

People have a tendency to settle for the first answer or alternative without really developing several answers or alternatives from which to choose. Developing several alternatives requires a combination of careful and thorough analysis, intuition, creativity, and a sense of humor. Several techniques using individual and group creativity are available to develop alternatives. These include brainstorming, synectics, and others, which are discussed later in the section.

Step 3: Selecting a Solution In this step, the various alternatives are evaluated against the established criteria for the solutions. In this way, the solution that best fits the criteria can be selected. Each alternative must be compared to others. Since "best" is a relative term, the alternative solutions must be evaluated to provide a reasonable balance of effectiveness and efficiency, considering the constraints and intangibles, if any.

If during this step the problem solver cannot establish a satisfactory solution, it may be necessary to return to Step 1 in order to redefine the problem or to repeat Step 2 in order to generate more realistic alternatives and solution criteria.

As part of the decision-making process, alternative solutions should be screened for the most appealing balance of effectiveness and efficiency in view of relevant constraints and intangibles. Russell Ackoff, a specialist in managerial problem solving, contends that three things can be done about problems: They can be resolved, solved, or dissolved (see Exhibit 5.16).

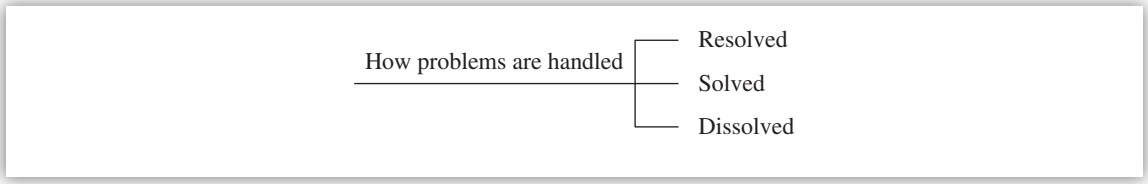


EXHIBIT 5.16 How Are Problems Handled?

Resolving the problem includes selecting a course of action that is good enough to meet the minimum constraints. Here the problem solver satisfices rather than optimizes. Optimizing or maximizing is selecting the best possible solution. When a problem is resolved by selecting a course of action that meets the minimum constraints, a manager is said to be satisficing. The manager uses a minimal amount of information to make a quick, good enough, and not the best, decision. Satisficing has been criticized as a shortsighted and passive technique emphasizing survival instead of growth. Idealizing involves dreaming that no problem would exist or changing the current situation so that the problem no longer exists.

SATISFICE VERSUS OPTIMIZE VERSUS IDEALIZE

- Satisfice is settling for a solution that is good enough.
- Optimize is systematically searching for a solution with the best combination of resources and benefits.
- Idealize is changing the nature of a problem's situation.

Solving the problem is when one selects the best possible solution with the best combination of benefits. A **problem is dissolved** when the situation in which it occurs is changed so that the problem no longer exists. Problem dissolvers are said to idealize because they actually change the nature of the system in which a problem resides.

RESOLVING VERSUS SOLVING VERSUS DISSOLVING

- Resolving the problem requires a qualitative, subjective approach.
- Solving the problem requires scientific observations and quantitative measurements.
- Dissolving the problem requires a combination of quantitative and qualitative tools.

Step 4: Implementing and Evaluating the Solution Once a solution has been chosen, implementation must be planned in detail. This step includes deciding who will do what and when. It requires implementation plans, checkpoints, schedules, and resources. The implementation of the action plan should have moved the situation from what is to what should be.

PROBLEM-SOLVING STRATEGY CHECKLIST

- Look for a pattern.
- Account for all possibilities.
- Act it out.
- Make a model or diagram.
- Work backward.
- Reason hypothetically.
- Restate the problem or change the problem representation (taking the point of view of an observer).
- Identify given, wanted, needed information.

At this point, both product and process evaluation are important. The outcomes must be measured against the desired criteria to determine if the goal has been reached and the problem solved. If people are still uncomfortable with the way things are, it may be necessary to start again at Step 1.

(C) Impediments to Problem Solving Business problems are solved either by individuals or by groups. The most neglected area of problem solving is human resources, the people who participate in the problem-solving group. The group leader can encourage new ideas and creativity in group members by following these guidelines.

- Practice effective listening because people think much more rapidly than they speak. Effective listening is the best way to gather information. Try not to be distracted.
- Practice "stroking," a concept borrowed from transactional analysis. A stroke is a unit of recognition. Provide recognition to people and ideas. Positive stroking makes people more important and secure and invites more ideas and creativity.
- Discourage "discounting" (i.e., not paying attention), another concept borrowed from transactional analysis. When discounting is high, group members will feel reluctant to respond to questions and will be constantly ready to attack or retreat. This is not a healthy climate for successful problem solving, and it encourages dysfunctional behavior and uncooperative attitudes among the members of the group.
- Keep the group members informed about progress and what is expected of them.

Reasons frequently cited by psychology researchers for people making mistakes in solving problems include lack of understanding of concepts, reasoning errors, failure to note details, and insufficient computation skills.[7] Researchers have identified these common traits that good problem solvers possess:

- Good estimation and analysis skills
- Ability to perceive similarities and differences
- Reflective and creative thinking
- Ability to visualize relationships

[7] *Problem Solving*, Vol. 2 (Columbus, OH: Ohio Department of Education, State Board of Education, 1980).

- Strong understanding of concepts and terms
- Ability to disregard irrelevant data
- Capability to switch methods easily, but not impulsively
- Ability to generalize on the basis of a few examples
- Ability to interpret quantitative data
- Strong self-esteem

A problem-solving attitude, an inquiring and questioning mind, can be developed. It does not occur by accepting from others truths and conclusions that the learner ought to establish by him- or herself. The attitude is produced by continued experience in solving real problems, one consequence of which is that the learner comes to expect new problems and to look for them. Auditors have the same agenda in mind. The ability to discriminate among possible alternatives is a valuable life skill. One should not think of problem-solving skills as a single, uniform capability. *Problems of different kinds may require substantially different problem-solving skills.*

Problem-solving expertise consists of skill in identifying obstacles that can be easily circumvented and of ingenuity in dealing with particular obstacles. The identification of problem obstacles is generally given too little priority because we are solution oriented. We spend too little time in exploring the problem situation.

IDEA GETTING VERSUS IDEA EVALUATION

- Reaching a final solution depends on both idea getting (generating alternatives) and idea evaluation (choosing the best alternative). Sometimes we do not achieve a satisfactory solution because we put too little effort into considering alternatives or we make a poor selection from those alternatives evaluated. Frequently the obstacle to successful problem solving is the tendency to evaluate and select an alternative before better ideas have been generated.
- Unless idea getting is stressed and idea evaluation temporarily suppressed, the presence of available alternatives can impede the possible consideration of other, more viable alternatives.

(D) Problem Solving and Creativity The reorganization of experience into new configurations is called "creativity." The best argument in favor of creativity is that environmental changes make creativity essential for long-term survival. Stagnation can lead to organizational failure or demise. Creativity is not easy to get or to manage, as it requires hiring intelligent people and motivating them to deliver to the fullest extent of their skills.

A creative act is one that is original, valuable, and suggests that the person performing the act has unusual mental abilities.[8] A creative act is a problem-solving act; in particular, it is the solution of an ill-defined problem. Four cognitive processes especially important for creativity include: (1) problem finding, (2) idea generation, (3) planning, and (4) preparation.

The discovery of a new problem not suggested by anyone else is important in any field. Three procedures that can help us to find problems are bug listing, searching for counterexamples, and searching for alternative interpretations.

[8] John R. Hayes, *The Complete Problem Solver,* 2nd ed. (Mahwah, NJ: Lawrence Erlbaum Associates, 1989).

Sometimes, when we are trying to solve an ill-defined problem, we are blocked by difficulty in generating ideas for solution. Brainstorming and discovering analogies may help us out of this difficulty. Planning is important in creative activities, as it is in any form of problem solving. Good writing and good art depend on good planning.

Internal auditors need to use creative skills during audit planning and the preliminary survey and during development of the audit program. Identification of audit objectives is important in the audit planning phase. Development of a good approach to conduct the preliminary survey requires creativity. Deciding what audit procedures need to be performed requires creativity during audit program development. Both new audits and repeat audits benefit from applying creative skills.

(E) Reasons Why Individuals Solve Problems Differently Problem-solving skills are different with different people. Five factors (see Exhibit 5.17) are key to a person's problem-solving capabilities:

1. Value system
2. Information filtration
3. Interpretation
4. Internal representation
5. External representation

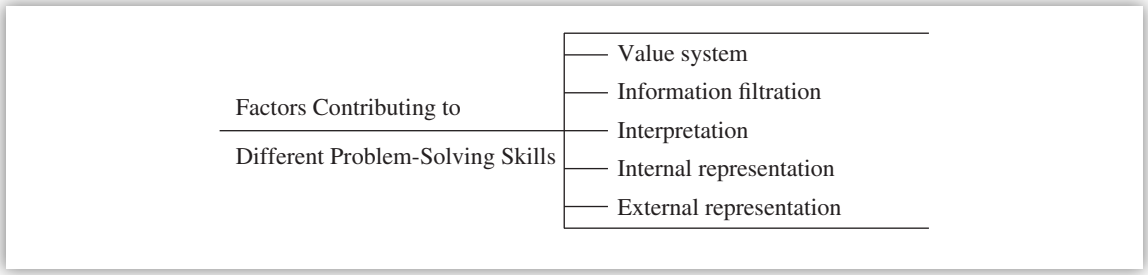


EXHIBIT 5.17 Factors Contributing to Different Problem-Solving Skills

Value System Individuals make decisions and solve problems differently due to our different value systems. If two people make different choices in the same situation, it does not mean that one of them is wrong; it may just be that they have different values. This means that we cannot tell how good people's decision-making processes are by the choices they make. However, training in formal decision-making methods and problem-solving skills would help. No matter what people's values are, if they use good decision-making methods, they should tend to agree with themselves when they make the same decision again.

Information Filtration Some people can filter relevant information from the irrelevant. It is a skill that can be acquired through reasoning and practice. Problem solving would be simpler for people who can think simply and clearly in their minds. Also, a multiple-level organization structure is most likely to produce information filtration. Information is subject to distortion or filtration as it moves through many channels of communication. The greater the level of communication, the greater the information filtration.

Even when two people represent the same problem, they may not represent it in the same way. A person who is very good at filtering out irrelevant details may produce a very sparse representation. Another person who is not good at filtering out irrelevant details may produce a complex and ornate representation.

Interpretation Forming a representation is a very active process in which a person adds and subtracts information and interprets information in the original situation. Pictures can be used during the process of interpretation.

Internal Representation Internal representation deals with analogies and schemas in our minds. When we encounter a problem, we recognize that we have seen a similar problem before. This is called "analogy." An example would be a car stalling and a similar audit situation. A problem schema is a package of information about the properties of a particular problem type. Problem schemas are an important part of the knowledge we use to solve problems.

INTERNAL REPRESENTATION OF A PROBLEM

Examples of internal representation of a problem include imaging, inferencing, decision making, and retrieving of knowledge from memory in an effort to understand the problem.

Our skill in problem solving depends in a very important way on our store of problem schemas. Each problem schema we know gives us a very valuable advantage in solving a whole class of problems—an advantage that may consist in knowing what to pay attention to, or how to represent the problem, or how to search for a solution, or all three. *Clearly, the more schemas we know, the better prepared we are as problem solvers.*

Different people may create different internal representations of the same problem. There are more differences between representations, though, than just the amount of detail they contain. One person may represent a problem in visual imagery, another in sentences, and a third in auditory images. If two people represent a problem in visual images, they may not use the same images. For example, people frequently use both auditory and visual imagery in solving arithmetic problems. While doing problems in their heads, people use visual images of the digits of the answer and of marks indicating borrowing or cancellation.

External Representation In many cases, an external representation is very helpful for solving problems. Drawing a sketch, jotting down lists, writing out equations, and making diagrams can help us to remember information and to notice new relations in the problem. Some relations in problems are easier to discover when diagrams are used. For example, a matrix representation is useful in solving control identification problems (e.g., matching controls to control objectives).

External representations are very helpful in solving complex problems, but they are not useful without an internal representation of the problem. An internal representation is essential for intelligent problem solving since it is the medium in which people think—the same way the words are the medium for speech. Sometimes an internal representation is sufficient for solving simple problems. However, external representation alone is not useful. Both representations are needed for most cases.

(F) Prospective and Retrospective Methods Often management asks auditors to deal with forward-looking, future-oriented problems or questions. Collectively they are referred to as prospective methods to distinguish them from approaches designed to answer questions about what is happening now or what has happened in the past—that is, retrospective methods. An auditor's problem-solving skill set should address both of these methods. Conducting a repeat audit of accounts payable is an example of a retrospective method. Performing a due diligence review is an example of a prospective method of problem solving.

EXAMPLES OF TYPES OF PROSPECTIVE METHODS

Four types of methods exist: actual, empirical, logical, and judgmental.

1. Actual types include experimental test and demonstration programs.
2. Empirical types include simulation and forecasting.
3. Logical types include front-end analysis, risk assessment, systems analysis, scenario building, and anticipatory analysis.
4. Judgmental types include Delphi techniques and expert opinion.

Basically, two types of forward-looking situations exist: anticipate the future or improve the future. In both situations, auditors would be critiquing others' analyses or would do their own analyses. Future needs, costs, and consequences are analyzed when anticipating the future issues. Courses of action that have the best potential for success are analyzed to improve the future. These types of questions are most appropriate in acquisition and divestiture audits.

The type of questions being addressed dictates the need for a systematic method of analysis. Where the questions are controversial, far-reaching, and sensitive, more systematic methods may be called for. Simple questions need simple methods. Some advantages of using systematic methods include: the full range of existing information can be brought to bear on the question and high-quality standards of evidence and analysis can be used in documenting the basis for answers about the future. Exhibit 5.18 compares retrospective methods with prospective methods.

Retrospective methods	Prospective methods
Require less judgment due to the lower level of uncertainty involved	Require more judgment due to higher degree of uncertainty involved
Decreased need for alternatives and options	Increased need for alternatives and options
Source of questions: existing criteria, issues, and policies	Sources of questions: ideas and assumptions about problems, probable causes, possible solutions
Primary sources of information: documents, administrative data, interviews, observations, surveys	Primary sources of information: prior research, theory, pilot tests, experimental tests of proposed approaches, expert opinions
Primary types of analysis: qualitative and quantitative approaches to empirical data, information syntheses in relation to criteria and issues	Primary types of analysis: simulations, forecasting, and information syntheses in relation to conceptual and operational assumptions of proposed solutions; Delphi techniques; analyses of likely effects

EXHIBIT 5.18 Comparison of Retrospective Methods with Prospective Methods of Problem Solving

(G) Tools and Techniques for Problem Solving Many tools and techniques are available for the problem solver to solve problems. They include brainstorming, synectics, nominal group technique, force-field approach, systems analysis, and others (see Exhibit 5.19).[9] Differences exist among the problem-solving methods, and all of them do not work equally well in different situations. In any given situation, one or two methods might have a greater probability of leading to the desired outcomes.

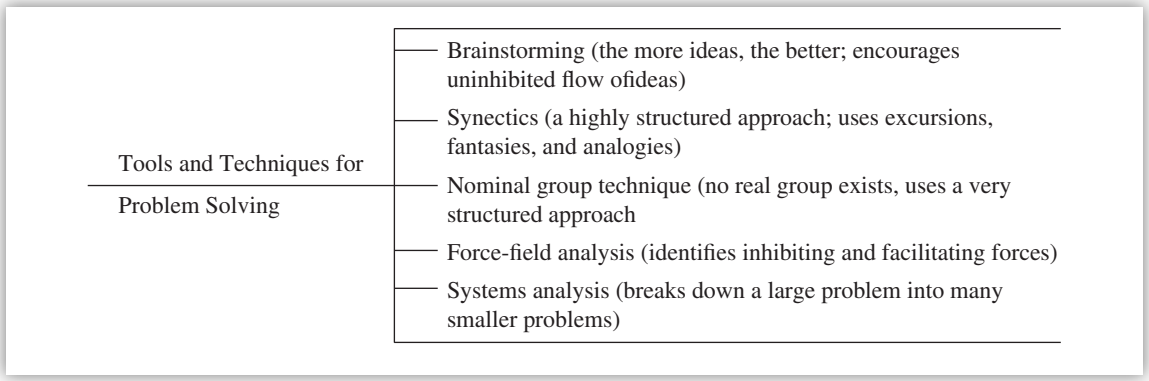


EXHIBIT 5.19 Tools and Techniques for Problem Solving

(H) Brainstorming The purpose of the brainstorming technique is to generate a great number of ideas; that is, its purpose is idea generation. The key is to let members of the group feel free to express whatever ideas come to mind without fear of judgment or criticism. Uninhibited flow of ideas is permitted; negative thinking is not permitted. Recording all ideas and deferring judgment until the later phases of the analysis is the hallmark of brainstorming. See Exhibit 5.20 for advantages and disadvantages of the brainstorming technique.

Advantages	Disadvantages
Rapid generation of ideas	Focuses on idea generation, not on specific solutions
Identification of many factors of a particular topic	Does not work well where problems are not open-ended
Expression of a cross section of views from various disciplines	

EXHIBIT 5.20 Advantages and Disadvantages of the Brainstorming Technique

The brainstorming technique is most effective when the presence of an expert is not necessary, the high level of creativity is seen as a bonus rather than an irritant, and a large quantity of ideas is needed.

MISCONCEPTIONS ABOUT BRAINSTORMING

There are two misconceptions about brainstorming: (1) there is a total lack of control and direction in a brainstorming session, and (2) brainstorming does not involve judgment or evaluation of ideas; all ideas are seen as equally effective and productive.

[9] Francis L. Ulschak, Leslie Nathanson, and Peter G. Gillan, *Small Group Problem Solving* (Reading, MA: Addison-Wesley, 1981).

There are four rules for effective brainstorming sessions.

1. **Postpone evaluation of ideas of others as well as one's own.** This rule is the most critical, because the best way to reduce effective idea generation is to make premature evaluations and/or judgments.
2. **"Freewheeling" is welcome and invited.** "Freewheeling" means that any idea is permitted, no matter how outlandish or fanciful. One person's flight of fantasy may be the trigger for another's generation of a very workable idea.
3. **Many ideas are wanted.** The greater the number of ideas, the greater the possibility that quality ideas will emerge.
4. **Encourage hitchhiking.** Hitchhiking is the art of combining and improving on ideas; in other words, building on another's suggestion. Frequently, a group will develop a cue for members to use when they want to hitchhike—for example, snapping a finger. Hitchhiking is a by-product of brainstorming.

(I) Synectics Synectics is a technique for creating an environment that encourages creative approaches to problem solving. It is a highly structured approach for an individual who needs a group to help solve a problem. *It involves the use of nontraditional activities, such as excursions and fantasies and analogies.* Synectics is good for idea generation and team building. See Exhibit 5.21 for advantages and disadvantages of the synectics technique.

Advantages	Disadvantages
The method works exceptionally well when people feel in a rut or blocked with a problem.	Participants may have difficulty with excursions; some may be reluctant to fantasize.
The process is fun—there is a lot of energy flowing.	The process works best with small groups of six to eight members.
It generates a great number of new perspectives on a problem.	The process works better for individual problems than for group problems.
In addition to structure, there is plenty of room for flexibility.	Although the process sounds easy, it requires much preparation.
Participants feel very involved in the process.	

EXHIBIT 5.21 Advantages and Disadvantages of the Synectics Technique

Excursions and fantasies are deliberate moves to get participants away from consciously thinking about the problem. In synectics, the excursion is used to involve the subconscious mind to work on the problem and find clues to possible solutions. Excursions are productive with regard to developing possible solutions, and they also serve to energize the group members.

Analogies are an important source of ideas when searching for problem solutions. A checklist is prepared for each type of analogy, including personal, direct, symbolic, fantasy, and attribute. The user works through the checklist and tries to find analogies of each type. Personal analogy is where the problem solver puts him- or herself directly into the problem situation. Direct analogy involves searching for a setting where the same function is accomplished.

Symbolic analogy is associated with symbols, notations, figures, and pictures. Fantasy analogy includes magic and science fiction. In an attribute analogy system, the checklist would list

attributes of an object—its name, form, function, color, and material. After listing the attributes, analogies are attached to each one by screening for useful insights. Analogies and symbols are also called free association, where unconventional thinking is encouraged.

(J) Nominal Group Technique The nominal group technique (NGT) is an idea-generating, consensus-building tool. *No real group exists—it is a group in name only.* A strength of this process is that it permits a problem to become focused in a short period of time. It uses a very structured approach and is an excellent technique to use when the group members are drawn from various levels of the organizational hierarchy or when they are in conflict with one another. The technique gives everyone an opportunity to express ideas without being interrupted by others in the group. See Exhibit 5.22 for advantages and disadvantages of NGT.

Advantages	Disadvantages
NGT can be used with groups of varying backgrounds, cultures, education, or work roles who share a common problem or goal.	The technique calls for a trained leader or group facilitator.
The technique can be used in groups where participants do not have previous training in group process or communication skills.	It can deal with only one question at a time.
The highly structured process is a quick way of bringing people together to approach a common task.	NGT is inappropriate to use in a group that does not already have interactive problem-solving and team-building skills.
NGT promotes the generation of many ideas surrounding an issue.	
NGT allows for maximum and equal participation of all group members, encouraging input from many areas of expertise.	
The NGT process is easy to run.	

EXHIBIT 5.22 Advantages and Disadvantages of the Nominal Group Technique

Social psychology researchers have found that individuals working in groups generate more ideas than when they work alone. Furthermore, nominal groups—groups in name only, where people are brought together but not allowed to communicate—have been found to be more effective for idea generation than interacting groups, where people meet to discuss, brainstorm, and exchange information. Such interacting groups tend to inhibit creative thinking. However, for purposes such as attitude change, team building, and consensus generation, interacting groups have been found superior.

BRAINSTORMING VERSUS SYNETICS VERSUS NOMINAL GROUP TECHNIQUE

- If the goal is idea generation, use brainstorming or synectics, since each facilitates more diverse or creative thinking.
- If the goal is for a group of relative strangers to meet in order to reach a group consensus concerning common issues, use the NGT since it is a structured process of consensus building.

The unique NGT process combines a silent time for idea generation with the social reinforcement of an interacting group setting. This structured process forces equality of participation among members in generating and sharing information about the issue. NGT groups may consist of five to eight participants.

(K) Force-Field Analysis Force-field analysis involves the identification of a problem, the factors or forces contributing to making it a problem, and steps for generating solutions. Two main sets of forces are identified: (1) inhibiting forces—those that resist the resolution of the problem; and (2) facilitating forces—those that push the problem toward resolution. Once the forces acting on a problem are identified, actions can be taken to decrease the major resisting forces, increase the major facilitating forces, or both. This process, then, is basically an analysis of the forces acting to keep the problem a problem. See Exhibit 5.23 for advantages and disadvantages of force-field analysis.

Advantages	Disadvantages
The outcome of the force-field analysis process is a detailed action plan with evaluation criteria built in.	The group may get lost in arguments about what the problem really is, what forces are the most important, which action steps to begin with, and so on.
It is an excellent process for a group to use in dealing with group problems.	Problems that are not easily and clearly defined many be difficult for this process.
It is an effective tool to define problems, analyze problems, and develop solutions into workable action plans.	The team leader needs to be a good listener and should be able to help the team weight and rank alternatives.
Group size is not a critical factor, and force-field analysis can be used as a team-building process.	

EXHIBIT 5.23 Advantages and Disadvantages of Force-Field Analysis

Force-field analysis calls for the definition of current conditions and desired conditions. Once a clear image of these conditions is established, effective intervention strategies can be devised to move from the present to the desired condition. As a problem-solving process, force-field analysis involves identifying and analyzing problems, developing strategies for change, and clarifying specific steps to be taken to confront the problem. It is an excellent analytical tool. The outcome will be a detailed action plan outlining when, to whom, and how the problem will be addressed. The force-field approach is useful for viewing a problem that involves the entire group, and it may be combined with other problem-solving methods in order to establish a long-term plan of action.

(L) Systems Analysis Systems analysis breaks down a large problem into many smaller problems. It is an excellent technique if the desired outcome of the problem-solving session is a detailed understanding of a problem. The technique offers a structure for analyzing a problem and various alternative solutions. However, it does not structure the roles of the participants. The major strength of this process is that it offers a method of reviewing the total context of a problem. The phrase "systems analysis" does not mean analysis of computer-based information systems. The scope is broader than that—manual, automated, or both. See Exhibit 5.24 for advantages and disadvantages of systems analysis.

Advantages	Disadvantages
The problem is fully analyzed, touching on important questions and areas of concern. Several alternatives are developed, leaving abundant options for choice. It can be combined with other problem-solving methods.	There may be a tendency for the group to get bogged down in the process.

EXHIBIT 5.24 Advantages and Disadvantages of Systems Analysis

This method requires the problem solver to look beyond the unit of the problem to the environment for various possible solutions. It focuses on three attributes: open systems, multiple reasons and causes, and the entire picture.

The first attribute of systems theory assumes that a system is open; it interacts with its environment and can be represented by three models: hierarchical, input-output, and entities model. In the hierarchical model, systems are seen within a structure of subsystems. This framework may be useful in identifying the context in which the group finds itself. An input-output model may be useful in identifying the inputs that are needed and how they are to be transformed toward the desired outputs. The entities model may be used to form tentative hypotheses about how the group members may interact.

The second attribute of systems theory looks at multiple reasons or causes for things; it keeps the problem solver from having tunnel vision concerning the nature of the problem. The systems approach moves away from linear causation, which assumes that the effects of a situation are based on single causes. Realizing that problems often have more than one cause helps the problem solver to attack the problem from several fronts.

The third attribute of the system model examines the entire picture rather than only one part or element. Remember the classic elephant story—different views of the elephant by six blind men.

(M) Considerations of Problem Solving: Traits and Behaviors All auditors should be familiar with certain traits and behaviors during problem solving. While certain problem-solving behaviors, such as conjecturing, predicting, and drawing conclusions, can be learned and taught, other behaviors and problem-solving traits, such as self-reliance, risk taking, creative thinking, and interacting, are examples of affective-related behaviors that are fostered through individual encouragement.[10]

An auditor needs to focus on the traits and behaviors listed next.

Traits

- **Curious.** Eager to investigate, to learn new approaches and techniques, to understand how a problem is solved.
- **Keen.** Interested in problems, quick to respond to individual challenges.
- **Interactive.** Participates freely with others, seeking and sharing ideas.

[10] *Problem Solving*, Vol. 2.

- **Creative.** Responds to problem situations in new or unusual ways; not confined in problem approaches or ways of thinking.
- **Receptive.** Willing to listen to and consider ideas of others.
- **Intuitive.** Able to act on hunches or educated guesses.
- **Retentive.** Draws on and applies previously acquired information in new situations.
- **Self-confident.** Believes that skills and abilities are adequate to meet the challenge of new problems.
- **Relishes challenges.** Desires and enjoys pitting abilities against problems.
- **Critical.** Evaluates ideas and explanations carefully; looks for exceptions to generalizations.
- **Organized.** Approaches problems systematically, investigates problem ideas in an orderly, sequential manner; keeps a record of successful and unsuccessful attempts.
- **Tolerant.** Listens to ideas and problem approaches that are not personal choices; willing to bide time in making and seeing suggestions acted on; respects problem-solving efforts and achievement of others.
- **Resourceful.** Able to overcome obstacles in more than one way.
- **Flexible.** Capable of changing or expanding thinking to incorporate new or different ideas from others.
- **Self-directed.** Motivated from within to pursue and continue with challenges.
- **Introspective.** Considers own thinking processes in problem solving; reflects on how new knowledge or discoveries integrate with previous information or thinking.
- **Risk taker.** Unafraid to be wrong in ideas or to be unsuccessful in efforts to solve a problem; willing to present ideas about a problem to others for evaluation.

Behaviors

- **Questions.** Expands on problem-solving discussion by asking about other cases, how the situation varies by changing givens; pursues matters that need clarification in own or others' thinking.
- **Notes details.** Considers all information that may affect the outcome of a problem; alert to recognizing relationships among variable quantities.
- **Discriminates.** Perceives similarities and differences among objects or relationships that are important to the problem; distinguishes relevant information from irrelevant problem material.
- **Recognizes patterns.** Detects similarities that characterize a set of information; able to predict missing elements.
- **Anticipates.** Examines alternatives using cause and effect reasoning without carrying action to conclusion; capable of meeting problems before they arise.
- **Predicts.** Foresees or foretells the outcomes of or results to a problem based on previous background, experience, or reasoning.
- **Generalizes.** Extends the results of a particular problem or set of data to a larger and more general situation.

- **Visualizes.** Forms mental images of problem variables to perceive interrelationships among them.
- **Infers.** Examines problem information carefully to derive hypotheses and draw conclusions.
- **Speculates.** Reflects on and reasons about problem components, interrelationships, and implications; forms educated conjectures from available evidence.
- **Concentrates.** Summons all of his or her skills and resources to attack a problem; overcomes extraneous influences and distractions.
- **Synthesizes.** Integrates individually acquired skills and information into a larger understanding of the processes and components of problem solving.
- **Draws conclusions.** Able to bring thinking to a decision to direct problem-solving actions; able to summarize the results of problems or implications.
- **Deliberates.** Recognizes the appropriate times to consider carefully the information of a problem before acting, the implications of a result before generalizing, the alternatives before choosing.
- **Perseveres.** Persists with a problem despite lack of success, discouragement, or opposition to his or her ideas; reluctant to give up on a problem.
- **Makes refined judgments.** Able to adjust thinking or statements based on additional information; able to improve the work of others by noting subtleties, distinctions, exceptions, or special cases.
- **Uses divergent thinking.** Able to perceive more than one implication or consequence to a problem action; able to consider unique or unusual approaches or outcomes to a problem; able to expand thinking throughout a problem rather than narrowing it.

(N) Problem Solving and the Internal Auditor: Applications Auditors solve problems when they engage in an audit. An example of a problem-solving skill required of internal auditors is that of determining which audit procedures are most appropriate for a given situation. Because internal auditing involves examining evidence and reaching conclusions based on that evidence, auditors must understand and be adept in the use of inductive reasoning. In addition, internal auditors must be able to evaluate a specific situation and deduce, for example, what evidence should be gathered to reach a valid conclusion. Several audit situations are presented to apply problem-solving skills.

- **Audit Situation No. 1.** An internal auditor wishes to determine whether the accounts payable ledgers accurately reflect the obligations of the firm to vendors. Goods are shipped FOB (freight on board) to the buyer's plant. The auditor needs to select the type of documents that provide the best evidence and are useful. Given documents such as vendors' packing slips, purchase orders, receiving reports, vendors' invoices, and purchase requisitions, the auditor would select purchase orders, receiving reports, and vendors' invoices.
- **Audit Situation No. 2.** During a preliminary survey of the accounts receivable function, an internal auditor discovered a potentially major control deficiency while preparing a flowchart. Since this is a major control problem, the auditor should take an immediate action by reporting it to the level of management responsible for corrective action and highlighting the control weakness to ensure that audit work steps to test it are included in the audit program.

- **Audit Situation No. 3.** An internal auditor observed that only one of the company's 10 divisions had a large number of material sales transactions close to the end of the fiscal year. In terms of risk analysis, this would most likely lead the auditor to conclude that there is a relatively higher risk of overstatement of revenues for this division than for other divisions.
- **Audit Situation No. 4.** During an audit for the state tax department, one of the audit objectives is to determine if reporting taxpayers are correctly disclosing their sales taxes. The audit procedure that would most effectively achieve that objective is to conduct field examinations of selected taxpayers.
- **Audit Situation No. 5.** Due to a widespread failure of department managers to meet their budgets, senior management has requested an internal audit of the budget process. The primary objective of such an audit would be to determine if budget-setting policies and procedures are adequate and are in use. The audit objective would not be whether individual variances are accurately reported or whether first-line managers are given an opportunity to provide inputs into their budgets.
- **Audit Situation No. 6.** One of the objectives of a computerized inventory system audit is to determine if merchandise levels are replenished on a timely basis. An appropriate audit procedure for this objective would involve detailed testing of the update program that creates new purchase orders. It would not involve an edit program that lists all quantities sold or batch totals for shipments or an update program that creates new part numbers.
- **Audit Situation No. 7.** To determine the sufficiency of evidence regarding interpretation of a contract, an auditor uses the best obtainable evidence, subjective judgments, objective evaluations, and logical relationships between evidence and issues.
- **Audit Situation No. 8.** While planning an audit, an internal auditor establishes audit objectives to describe what is to be accomplished. A key issue to consider in developing audit objectives is the auditee's objectives and control structure. The qualifications of the audit staff selected for the engagement, recommendations of the auditee's employees, or the recipients of the audit report are not key issues.
- **Audit Situation No. 9.** When receiving materials, reports are forwarded to the purchasing department where they are matched to purchase orders and then sent to accounts payable. This is a problem situation that should cause the auditor to question the adequacy of internal controls in a purchasing function. The problem is solved when the accounts payable department receives all receiving reports directly, matches them to purchase orders, and prepares payments.
- **Audit Situation No. 10.** In an audit of an automated inventory control system, the audit approach that would provide the best evidence that purchase orders are authorized is testing to ensure that only authorized persons are able to change parameters in the computer program that generates purchase orders. Tracing purchase orders to the computer listing, comparing receiving reports with purchase order details, or reviewing system documentation to determine proper functioning of the program would not provide the best evidence.
- **Audit Situation No. 11.** A company manufacturing special-order products is experiencing excessive rates of rejection of finished products. An audit procedure to identify the source of the problem is evaluating communication from the sales department to the production department. Evaluating communication from the production department to the sales department, analyzing customer demand for the product, or testing whether supply of the product is sufficient to meet customer demand would not identify the source of the problem.

- **Audit Situation No. 12.** An internal auditor is planning an operational audit of the traffic department. The audit objective that best describes the focus of the audit would be to verify that the selection of carriers and routes provides the most economical and timely shipments of supplies and finished goods. The objective would not be to determine the market potential for the company's products, determine that the proper goods and services are obtained at the right price, or ensure that distributors give extra attention to sales of the company's products.
- **Audit Situation No. 13.** An audit of the purchasing function disclosed that orders were placed for materials that at that time were being disposed of as surplus. The best solution to this problem would be a recommendation to develop and distribute periodic reports of surplus stocks. The solution would not involve having all purchase requisitions approved by the responsible purchasing agent, scheduling purchases based on past orders placed, or employing a historical reorder point system.
- **Audit Situation No. 14.** An internal auditor is evaluating the propriety of a payment to a consultant. The most appropriate evidence for the auditor to obtain and review would be documentary evidence in the form of a contract. It would not be oral evidence in the form of opinions of operating management, analytical evidence in the form of comparisons with prior years' expenditures on consultants, or physical evidence in the form of the consultant's report.
- **Audit Situation No. 15.** An internal auditor is evaluating the reasonableness of account balances. The most relevant form of evidence to obtain to achieve this audit objective would be analytical evidence, not documentary, physical, or testimonial evidence.
- **Audit Situation No. 16.** A large public charity raises funds for medical research from the general public by using a wide variety of solicitation techniques. In an audit of donations, the auditor would select these audit procedures: written confirmation of a sample of direct mail pledges, reconciliation of depository bank accounts, and reconciliation of raffle tickets sold to amounts deposited in the bank. The auditor would not select "Surprise observation of door-to-door solicitation teams" since it is not an effective audit procedure.
- **Audit Situation No. 17.** A large hospital is faced with quality problems in housekeeping services. The most reliable source of information for an auditor to evaluate the quality of such services would be to interview a sample of medical personnel since they can give firsthand information about quality problems. The following sources would not provide reliable information since they would not be objective: scrutiny of survey forms returned by medical personnel directly to the administrator of the hospital (medical personnel may be inhibited from telling the truth to the administrator); a review of records maintained by the medical records department of the hospital; and a personal interview with the dean of the school of medicine that is affiliated with the hospital (the dean would not be close to the action).
- **Audit Situation No. 18.** One payroll audit objective is to determine whether employees received pay in amounts recorded in the payroll journal. The auditor needs to select an audit procedure that would achieve the audit objective. Comparing the canceled payroll checks to the payroll journal would be the best audit procedure since the endorsement on the back of the check is an indication of the right employee receiving the amount. These audit procedures would not be meaningful to use: reconciling the payroll bank account, requesting that a company official distribute all paychecks, or determining whether a proper segregation of duties exists between recording payroll and reconciling the payroll bank account.

- **Audit Situation No. 19.** The auditor is evaluating the adequacy of a company's insurance coverage. The auditor developed a detailed schedule of current insurance policies in force. The most likely source of information for the working paper would be the files containing insurance policies with various carriers. These sources would not be appropriate: original journal entries found in the cash disbursements journal and supported by canceled check; management's charter prescribing the insurance staff objectives, authority, and responsibilities; or the current fiscal year's budget for prepaid insurance together with the beginning balance sheet amount.
- **Audit Situation No. 20.** In examining whether an auditee is conforming to the company's affirmative action policy, the internal auditor has found that 5% of the employees are from minority groups, and no one from a minority group has been hired this year. The most appropriate conclusion the auditor should draw is that insufficient evidence exists of compliance with the affirmative action policy. The reason for insufficient evidence is that the target percentage of minority hiring is not known and how many total employees were hired this year is not known.
- **Audit Situation No. 21.** During an early phase of an extensive audit of a manufacturing company's inventory management system, an auditor discovered that there had been recurring stock-outs for some high-demand items and that this had led to expensive expediting and work stoppages. Further investigation revealed that the purchasing department had regularly ordered these items based on purchase orders produced automatically by the computerized inventory system. The quantity ordered had been based on an EOQ model included in the computerized inventory system. The auditor determined that the EOQ model was properly designed and that the problem had resulted from failure to update data in the model concerning the time required for delivery. The auditor is now faced with selecting an appropriate action to resolve the problem at hand. Some examples are presented next.
  - The auditor would most likely conclude that these facts indicate an important problem that should be included in the audit report.
  - If the auditor decided that the situation warranted management's immediate attention and the entire audit would not be completed for several weeks, communication with management would probably take the form of a written interim report to operating management. An oral report would not be proper since statistics and facts may be presented that require a written document.
  - The importance of the problem outlined would probably cause the auditing department to follow up on action taken by management as a result of an audit communication. Follow-up should be conducted by scheduling a review of this area in the near future.
- **Audit Situation No. 22.** A company has computerized sales and cash receipts journals. The computer programs for these journals have been properly debugged (i.e., tested). The auditor discovered that the total of the accounts receivable subsidiary accounts differs materially from the accounts receivable control account. A reason for this problem could be that credit memoranda are being improperly recorded. These would not be good reasons for causing the problem: lapping of receivables, receivables not being properly aged, and statements being intercepted prior to mailing.
- **Audit Situation No. 23.** An auditor performing a payroll audit wants to be assured that persons for whom paychecks are produced actually exist and are employees of the organization. The most appropriate evidence to achieve these objectives would be visual or physical evidence obtained by observing the distribution of paychecks. This evidence is more direct and firsthand. This evidence would not be appropriate: documentary evidence in the form

of time cards signed by supervisors, documentary evidence in the form of personnel and payroll records, or oral evidence obtained by discussions with supervisors and payroll clerks. Fraud could be present in these three procedures.

- **Audit Situation No. 24.** An auditor is testing for the misclassification of capital acquisitions as expenditures. The most efficient testing procedures would be to scan the repair and maintenance records and investigate large-dollar-value entries. There is a tendency to misclassify high-dollar-value items instead of low-dollar-value items to obtain big impact. These testing procedures would not be efficient: taking a physical tour of plant facilities before starting an audit, reviewing company capital-acquisition policies with purchasing personnel, or tracing capital additions back to source documents.
- **Audit Situation No. 25.** A machinist claims that his poor-quality output is due to a contracted maintenance service employee's failure to perform required service on his equipment. The most convincing evidence for the auditor to determine whether the service was performed is whether the shop supervisor initialed the serviceperson's work order for the work in question. These items would not provide convincing evidence: a label attached to the equipment has checkmarks showing the maintenance work was performed on the scheduled dates, the maintenance service's invoice listing the equipment in question was paid, or the plant engineer's approval of the listed services as adequate for the equipment.
- **Audit Situation No. 26.** An auditor's objective is to verify ownership of selected vehicles. The best source of evidence would be vehicle titles and current license certificates since they are official documents. These items would not provide best source of evidence because they cannot be relied on: property records containing vehicle identification numbers, properly approved purchase orders, or invoices from dealers.
- **Audit Situation No. 27.** An auditor who wishes to substantiate the gross balance of the account "Trade Notes Receivable" is considering the advisability of performing these four procedures.

  1. Age the receivables.

  2. Confirm the notes with the makers.

  3. Inspect the notes.

  4. Trace a sample of postings from the sales journal to the notes receivable ledger.

  The auditor needs to select appropriate audit procedures to meet the objective. The auditor would select procedures 2 and 3 to accomplish the objective.
- **Audit Situation No. 28.** The audit objective is to determine that nonrecurring purchases, initiated by various user organizations, have been properly authorized. All purchases are made through the purchasing department. The auditor would select purchase requisitions for tracing purchases since they provide a starting point for purchases. Other documents, such as purchase orders, invoices, and receiving reports, would not help in achieving the audit objective since they come after purchase requisitions.
- **Audit Situation No. 29.** A large university has relatively poor internal accounting control—a problem. The university's auditor seeks assurance that all tuition revenue has been recorded. The auditor could best obtain the desired assurance by comparing business office revenue records with registrar's office records of students enrolled since they provide a direct link. These audit procedures would not solve the problem: confirming a sample of tuition payments with the students, observing tuition payment procedures on a surprise basis, or preparing year-end bank reconciliation.

- **Audit Situation No. 30.** A company invests material amounts of idle cash in marketable securities. The auditor has reason to believe that suboptimal use (a problem) is being made of the idle cash. The audit procedure that would provide the most reliable evidence is computation of the rate of return earned on investments and comparison with alternative investments.

  Analytical evidence is being sought here in order to obtain a feel for the reasonableness of investments and returns. These audit procedures would not provide reliable evidence: review of the minutes of the company's investment committee; confirmation of security transactions, and income received, with the company's independent stockbrokers; or comparison of actual with budgeted investment income earned. These three procedures do not provide solid evidence.

- **Audit Situation No. 31.** An audit discloses payments for unauthorized purchases. The auditor needs to recommend specific control procedures that require management's closer attention. The auditor would recommend approval of purchase requisitions and purchase orders since this is a preventive control procedure. The auditor would not recommend these control procedures: verification of agreement of voucher with invoice, comparison of invoice with receiving report, or comparison of voucher with supporting invoices by check signers. These three procedures are detective control procedures and do not help in controlling unauthorized purchases.

(ii) Decision Making

In this section, we first discuss the theory behind decision making, followed by its application to internal auditing. Decision making is a process of choosing among alternative courses of action. The correct sequence of the decision-making process is shown in Exhibit 5.25.

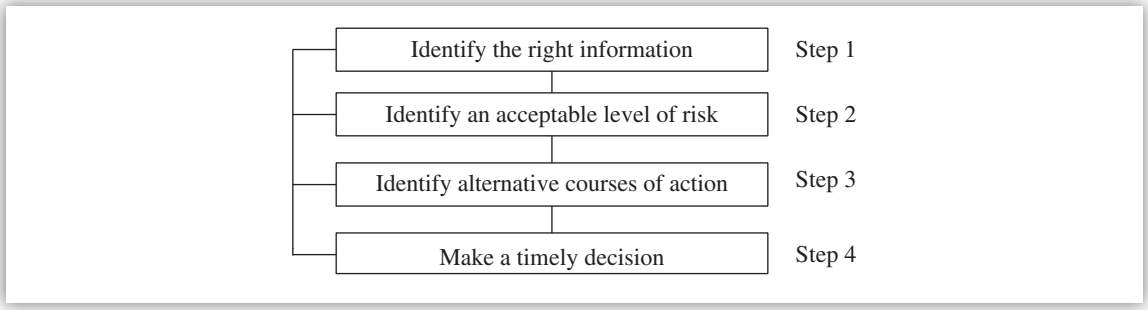


EXHIBIT 5.25 Steps in the Decision-Making Process

Note the difference between problem-solving and decision-making steps. Identify an acceptable level of risk (Step 2) does not enter into the problem-solving process. Risk is unique to decision making and is an integral part of it. Decision making reduces or increases the risk, depending on the quality of the decision making and the level of uncertainty.

The process of management is fundamentally a process of decision making. The functions of management (planning, organizing, directing, and controlling) all involve the process of initiating, selecting, and evaluating courses of action. Therefore, decision making at the center of the functions comprises the management process. The manager makes decisions in establishing objectives: planning decisions, organizing decisions, motivating decisions, and control decisions.

Professor Igor Ansoff classifies the organizational decisions into three categories: strategic decisions, administrative decisions, and operating decisions (see Exhibit 5.26).[11]

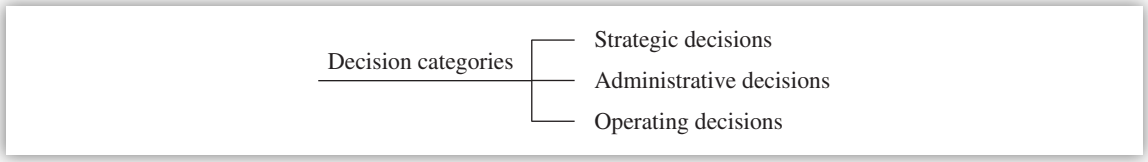


EXHIBIT 5.26 Decision Categories

Strategic decisions are primarily concerned with the external rather than the internal problems of the firm. Examples include product mix and markets to sell.

Administrative decisions are concerned with structuring the firm's resources to create maximum performance potential.

Administrative decisions are further divided into organizational structure and resource acquisition and development. Organizational structure involves structuring of authority and responsibility relationships, work flows, information flows, distribution channels, and location of facilities. Resource acquisition and development involves the development of raw material sources, personnel training, personnel development, financing, acquisition of facilities, and equipment.

Operating decisions are primarily concerned with maximizing the profitability of current operations. They include pricing, establishing market strategy, setting production schedules and inventory levels, and deciding on the relative expenditures in support of R&D, marketing, and operations.

Basically, a decision must be made when the organization faces a problem, when it is dissatisfied with existing conditions, or when it is given a choice. There is no unified agreed-on structure for decision theory because each decision maker has a different value system. A significant amount of work is performed by staff and line people in discovering problems, defining the problems, and preparing the alternatives for decisions. The actual decision is only the conclusion of a decision-making process. The intelligence phase in the decision-making process includes finding the problem.

The three-step sequence of setting objectives is listed next.

1. Broad objectives are established at the senior managerial levels.
2. Strategies and department goals are developed from the broad objectives. The department goals provide a framework for decision making at lower managerial levels.
3. The manager needs to balance multiple objectives, conflicting objectives, and the hierarchy of objectives.

As the name indicates, the term "multiple objectives" means that the manager is focusing on two or more objectives at the same time. Examples include market growth, diversification, profit/sales maximization, employee attitudes, social responsibility, and employee development. Quantification is difficult to obtain on the latter three objectives.

[11] Igor H. Ansoff, *Corporate Strategy* (New York: McGraw-Hill, 1965).

Conflicting objectives arise when two objectives are at odds with each other. For example, social responsibility, such as pollution control projects, may adversely affect profit margins.

Hierarchy of objectives means that objectives of organizational units must be consistent with the objectives of higher organizational units. This means there are objectives within objectives. If the cascade of organizational objectives is not consistent, suboptimization results. It occurs where a departmental level maximizes its own objectives but, in doing so, subverts the overall objectives of the organization. Examples include dichotomies where the sales manager prefers large inventories; the production manager prefers large production runs; the warehouse manager prefers minimum inventory; the purchasing agent prefers large lot purchases; and the financing manager prefers low inventories, low production runs, and so on.

(A) Many Facets of Decision Making Managers and leaders make decisions. The type of decision made depends on the level of that manager in the organization hierarchy. To accommodate this diversity, many facets of decision making exist, as depicted in Exhibit 5.27.

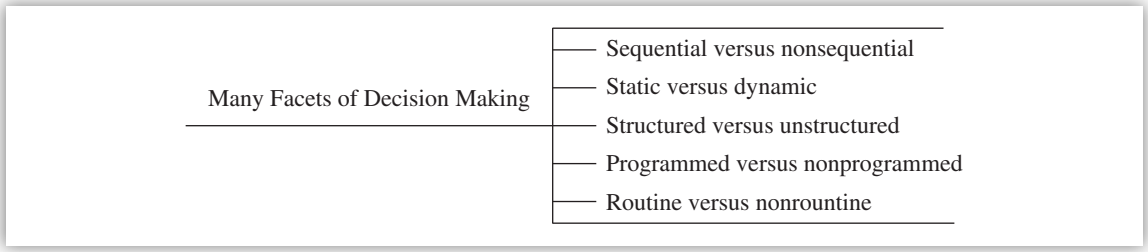


EXHIBIT 5.27 Many Facets of Decision Making

Sequential/Nonsequential Decision Making Sequential decision making is the process of successively solving interrelated subproblems that make up a large complex problem. It uses the principle of divide and conquer. Decision C cannot be made until decisions A and B are made. Most of senior managements' decisions are nonsequential in nature for strategic issues; lower-level management mostly makes sequential decisions.

DECISION RULES

Decision rules are behind the programmed decisions procedures. Decision rules require that there is a standard approach to resolve recurring problems and that the problems need to be solved only once.

There are no decision rules behind nonprogrammed decision making. Every situation is different, unique, and complex, requiring innovative and creative problem-solving approaches.

Static/Dynamic Decision Making Static decisions are onetime events leading to one-shot decisions. Dynamic decision making emphasizes that management's decisions are not usually one-time events but are successive over a time frame. Future management decisions are influenced to some degree by past decisions.

Structured/Unstructured Decision Making Structured decisions have formal rules while unstructured decisions have no rules. Examples of structured decisions include production

scheduling, inventory reordering, and materials requirements planning. These models have a rigid structure to the decision processes and are programmed to perform routinely without much human involvement. Examples of unstructured decision models include decision support systems and executive support systems. All decision models are rational within their own limits and boundaries. Structured decisions can mean programmed decision making; unstructured decisions can mean nonprogrammed decision making.

Programmed/Nonprogrammed Decision Making Programmed decisions are those that are repetitive and routine, requiring definite procedures. Examples of programmed decisions are employee hiring decisions, billing decisions, supply order decisions, consumer loan decisions, and pricing decisions. In contrast, nonprogrammed decisions are unstructured and novel; there are no set patterns for handling them. Higher levels of management are associated with the unstructured, nonprogrammed decisions.

Nonprogrammed decisions are complex, important situations, often under new and unfamiliar circumstances. Nonprogrammed decisions are made much less frequently than are programmed decisions. Examples of nonprogrammed decisions include building a new manufacturing plant or warehouse, and merger and acquisition decisions. There is no cut-and-dried method for handling nonprogrammed decisions because the problem has not arisen before, or because its precise nature and structure are not clear, or because it is so important that it deserves a custom-tailored approach. See Exhibit 5.28 for a hierarchy of management decision making.

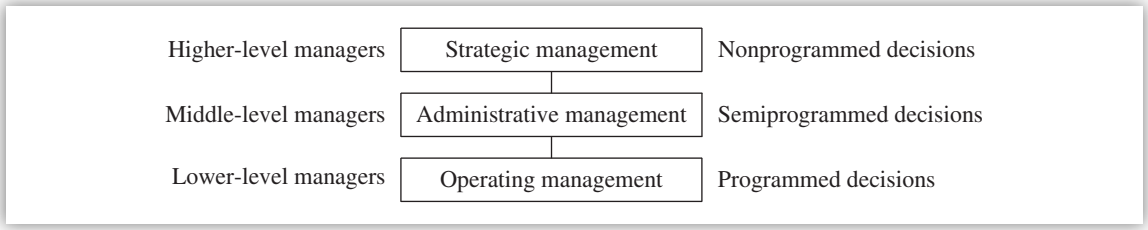


EXHIBIT 5.28 Hierarchy of Management Decision Making

Senior-level managers make nonprogrammed (nonroutine) decisions for strategic management purposes. Programmed (routine) decision address lower-level and highly repetitive tasks, as they are fully programmed. Clerks and computers are involved in routine programmed decisions, such as production scheduling and machine loading. Programmed decisions serve the needs of operating management. However, there is an overlap with semiprogrammed decisions in the sense that such decisions are made by both higher-level managers and middle-level managers.

The Institute of Management Accountant's research study identified nine models to describe nonroutine decision-making environments and labeled them as semiprogrammed decisions.[12] The nine decision models are listed next.

1. New product decision
2. Distribution channels decision

[12] *World-Class Accounting for World-Class Manufacturing* (Montvale, NJ: Institute of Management Accountants, 1990).

3. Acquisition decision
4. Divestment (product abandonment) decision
5. Capital expenditure decision
6. Make-or-buy decision
7. Lease-or-buy decision
8. Pricing decision
9. Manpower planning decision

Routine/Nonroutine Decision Making Routine decisions involve structured and programmed tasks. Nonroutine decisions involve unstructured and nonprogrammed tasks. Higher levels of management deal with nonroutine decision making while lower-level management handles routine decisions. Exhibit 5.29 depicts who makes what decisions.

Type of decision	Lower-level management	Higher-level management
Sequential decisions	x	
Nonsequential decisions		x
Structured decisions	x	
Unstructured decisions		x
Programmed decisions	x	
Nonprogrammed decisions		x
Routine decisions	x	
Nonroutine decisions		x

EXHIBIT 5.29 Who Makes What Decisions?

(B) Decision-Making Models Models are predetermined procedures that specify the step-by-step actions to be taken in a particular situation. Two types of decision models exist: normative and empirical models. Normative models prescribe the decision-making process—what should be. These models do not describe actual management practice in decision making. Instead, they describe how a decision procedure should be followed.

Empirical decision models do not describe how a decision maker should go about making a decision. Instead, they describe the actual decision processes followed by a decision maker—what is. A decision process is any interrelated set of activities leading to a "decision"—a commitment of resources. Reconciliation is needed between the normative and descriptive results in order to develop theories and hypotheses about how managers make use of information. *When there is no set of procedures for a decision process, then by definition there is no model for it. Examples include crisis handling and leadership.*

Normative models are programmed decisions. They help lower-level operating management to implement programs such as production scheduling or inventory control. Empirical models are nonprogrammed decisions. They help middle to senior management in making strategic decisions such as pricing and new product introduction.

NORMATIVE MODEL VERSUS EMPIRICAL MODELS

- Normative models are prescriptive in nature, address what and how it should be, and are programmed.
- Empirical models are descriptive in nature, address what is, and are nonprogrammed.

(C) Types of Data Used in Decision Making Decision making is a process that incorporates the estimating and predicting of the outcome of future events. When specific events are known with certainty, the decision maker does not use probabilities in the evaluation of alternatives. When specific events are uncertain, the decision maker uses probabilities in the evaluation of alternatives. The decision maker often uses the most likely outcome stated in deterministic format rather than incorporating all outcomes in a probabilistic (stochastic) format.

A decision maker uses two types of data: deterministic data and probabilistic data. Deterministic data are known and not subject to any error or distribution of error. They are based on historical data; their environment is stable and predictable. Decision results will be certain with a single unique payoff. There is only a single outcome for each possible action.

Probabilistic data is used by the decision maker to evaluate decisions under situations of risk and uncertainty. An estimation of distribution of possible outcomes can be made, not an assured or a predictable outcome. The environment is characterized as unstable and unpredictable since each event is assigned a probability of occurrence. Probabilistic data allows for better risk evaluation since sensitivity analysis can be performed on each action to measure the material impact of the various events.

An estimated payoff table or decision tree can be developed for analysis. A drawback of using probabilistic data is the availability and integrity of data to determine multiple courses of action.

DETERMINISTIC DATA VERSUS PROBABILISTIC DATA

- Deterministic data are known, and the environment is stable and predictable.
- Probabilistic data are not known, and the environment is unstable and unpredictable.

(D) Types of Decisions Decision making is a frequent and important human activity and is especially a managerial activity. Decisions are not all of one kind. The procedure for making one decision, such as buying a home, is entirely different from making another decision, such as taking a CIA examination.

Decision making is related to risk levels. With respect to risk, individuals act differently and can be grouped into three categories: risk takers, risk neutral, and risk averters. When contrasted with a risk-taking entrepreneur, a professional manager (or an auditor) is likely to be more cautious as a risk taker (i.e., either risk neutral or risk averter). Another factor is that risks are related to returns. The higher the risk, the greater the return, and vice versa. Also, controls are related to risks. The higher the risk, the greater the need for controls, and vice versa. Controls reduce or eliminate risks and exposures.

Four general types of decisions exist that require different decision procedures: (1) decisions under certainty, (2) decisions under risk, (3) decisions under uncertainty, and (4) decisions under conflict or competition (see Exhibit 5.30).

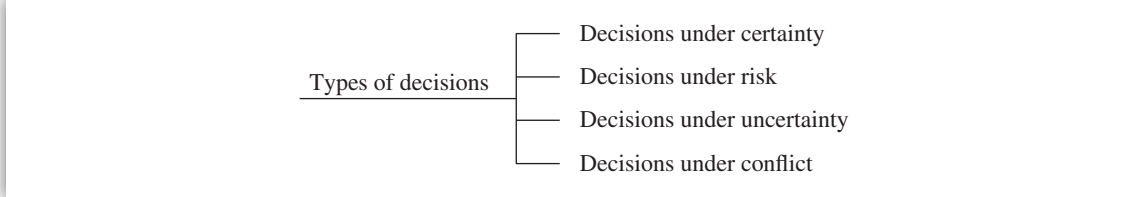


EXHIBIT 5.30 Types of Decisions

Decision Making under Certainty A decision maker is operating in an environment where all of the facts surrounding a decision are known exactly, and each alternative is associated with only one possible outcome. The environment is known as certainty.

Five different methods exist that are useful for making decisions under certainty. The first four methods are optimization methods—that is, they attempt to identify the very best alternative available. The fifth method, satisficing, simply looks for the first satisfactory alternative (see Exhibit 5.31).

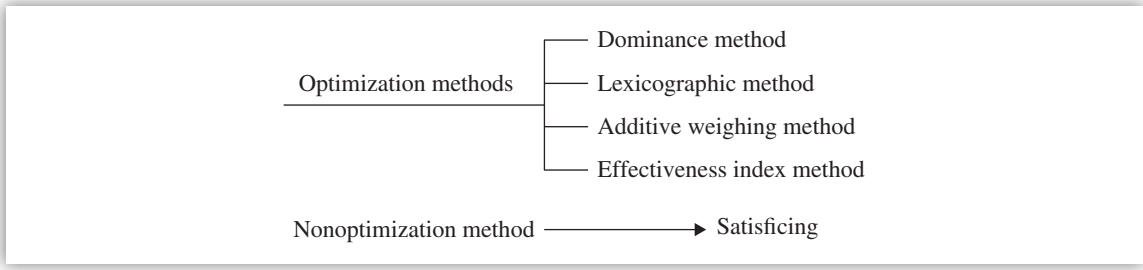


EXHIBIT 5.31 Optimization Methods

The **dominance method** is the simplest of the decision procedures. To use it in making decisions, it is necessary to find the dominance relations among the alternatives. One alternative dominates another if both of the following are satisfied:

1. It is at least as good as the other on all properties, and
2. It is better on at least one property.

Any alternative that is dominated by another is dropped from consideration since it will never be judged the best alternative by any reasonable decision procedure. Any alternative that dominates all the others is chosen as best.

VALUE SYSTEM IN DECISION-MAKING CHOICES

- If two people make different choices in the same situation, it does not mean that one of them is wrong; it may just be that they have different values. Therefore, the correct choice in any decision-making situation depends on the decision maker's individual value system.
- Generating alternatives, examining their properties, and choosing among the alternatives are all activities that may add considerable cost to the decision-making process.

The advantage of the dominance method is that people can agree about which alternatives are dominant. It is easy to apply, and its results are reliable. The disadvantages of this method are that it is not a powerful decision-making method because it usually does not eliminate very many of the alternatives. Examples of applications of decision making under certainty are linear programming, transportation problems, inventory models, and break-even analysis.

The **lexicographic method** is so named because of its resemblance to the procedure for ordering the definitions of words in the dictionary. In this method, look first at the most important the definitions of. If two alternatives have the same value on this property, then decide on the basis of the second most important property, and so on. It is necessary to specify the order of importance of the properties of the alternatives.

To make a decision by this method, consider the most important property first. If one alternative is better than the other alternatives on the most important property, then that alternative is the one chosen. If two or more alternatives are tied on the most important property, then drop the other alternatives from consideration and consider the next most important property in order to break ties. If any ties remain unbroken, then consider the third property, and so on. Changing the order of importance of the properties in the lexicographic method does not always change the alternative chosen as best.

The lexicographic method is most appropriate when one of the properties outweighs all of the others in importance. The method's major strengths under these circumstances are that it is quick and easy to apply. This method is least appropriate when the properties are roughly equal in importance. Under these circumstances, the method may lead us to choose an alternative that has a slight advantage in the most important property, even though that advantage is outweighed by big disadvantages in other properties. This happens because the lexicographic method typically ignores all but the most important property.

The **additive weighing method** takes all of the properties into account but does not give them equal weight. The more important properties receive heavy weights and the less important ones lighter weights. To use this method, numbers both for weights of the properties and for the values of the properties reflecting values to the decision maker must be available.

To make a decision by the additive weighing method, multiply numerical values of the properties by the weights of the properties for each alternative. Then choose the alternative with the largest sum as "best." This method takes all of the properties into account in making the decision but does not take the interactions of the properties into account. Therefore, this method can lead to inappropriate decisions by ignoring these interactions, just as the lexicographic method can lead to inappropriate decisions by ignoring the less important properties. The major drawback of this method is that it is time consuming and it is difficult to obtain the numbers for the weights and values of the properties.

USE OF DECISION-MAKING METHODS

Decision methods such as lexicography and additive weighing are useful because they allow people to substitute reliable objective procedures for unreliable subjective ones.

The **effectiveness index method** takes into account the interactions that the additive weighing method ignores. This method is used when the interactions are especially strong or because errors in decisions are very costly, or both. This method requires an extensive analysis of the situation under consideration, and designing and implementing such a method is very expensive and time consuming.

Satisficing is a nonoptimizing approach to decision making under certainty. The satisficing method requires the decision maker to identify the worst value he or she is willing to accept for each of the attributes. The decision maker then considers all of the alternatives in order, rejecting any alternatives that fall below the minimal values of the attributes and accepting the first alternative that meets all of the minimal values.

The satisficing method is particularly useful when we have to choose among a very large number of alternatives and it is not necessary to find the best. This method is less costly since it does not examine all of the alternatives and may not yield a decision at all if the decision-making standards are very high.

KEY CONCEPTS TO REMEMBER: Decision Making under Certainty

- All optimizing methods are designed to find the best available alternative and are suitable for idealized situations. They examine all alternatives available.
- The nonoptimizing method is not designed to identify the best alternative. Rather, it is designed to find the first satisfactory alternative that is more suitable to real-world situations. Only some alternatives are examined.

Decision Making under Risk When a decision maker is faced with a decision and the probabilities of various outcomes are known, the situation is said to be decision making under risk (see Exhibit 5.32). Gambling decisions are typical of decisions under risk. An essential feature of decisions under risk is that we can calculate a probability for the effect of the chance event. Tossing a fair coin, rotating a roulette wheel, and rolling a die are examples of decisions under risk. Examples of decision making under risk can be found in queuing theory, statistical quality control, acceptance sampling, PERT, and so on. Decision trees are used to assist the decision maker under conditions of risk.

EXHIBIT 5.32 Perfect Certainty versus Risk versus Perfect Uncertainty

Risk is a condition faced by managers when they have to make a decision based on incomplete but reliable information. Uncertain conditions exist when little or no reliable information is available. Certainty conditions exist when complete, reliable information is available.

One widely recommended technique for making risky decisions is to choose the action that has the greatest expected value. The expected value of an action is the average payoff value we can expect if we repeat the action many times.

Example of Expected Value

Game 1. Win $2.00 whether the coin comes up heads or tails when a fair coin is tossed.

Game 2. Win $10.00 if the coin comes up heads and lose $5.00 if it comes up tails.

$$\text{Expected value} = \text{Average payoff} = \text{Probability of a head } (PH) \times \text{Payoff for heads } (VH) + \text{Probability of a tail } (PT) \times \text{Payoff for tails } (VT)$$

$$EV = PH \times VH + PT \times VT$$

Here *PH* and *PT* have equal chances, that is, 1/2.

$$EV \text{ (for game 2)} = 1/2\ (10.00) + 1/2\ (-5.00) = 5.00 - 2.50 = 2.50$$

$$EV \text{ (for game 1)} = 1/2\ (2.00) + 1/2\ (2.00) = 1.00 + 1.00 = 2.00$$

Since the expected value of game 2 is greater than the expected value of game 1, we should choose game 2 in order to maximize our expected value. Whether we choose to play game 1 or 2 depends on whether we are risk averse or not. Game 1 is a no-lose game while game 2 is not.

Decision Making under Uncertainty Like decisions under risk, decisions under uncertainty involve a chance factor. The unique feature of decisions under uncertainty is that we cannot calculate a probability for the effect of the chance event. This is a situation in which a decision must be made on the basis of little or no reliable factual information. When considering pricing of competitors, actions of regulatory agencies, and strikes of suppliers, the decision maker is addressing the problem of uncertainty.

Multiple outcomes are possible. The first task is to establish subjective probabilities of occurrence for the multiple outcomes. Under conditions of uncertainty, the rational, economic decision maker will use expected monetary value as the decision criteria. The expected monetary value of an act is the sum of the conditional profit (loss) of each event times the probability of each event occurring.

Four strategies for making decisions under uncertainty include: (1) the mini-max strategy, (2) the maxi-max strategy, (3) the Hurwicz strategy, and (4) and the mini-max regret strategy (see Exhibit 5.33).

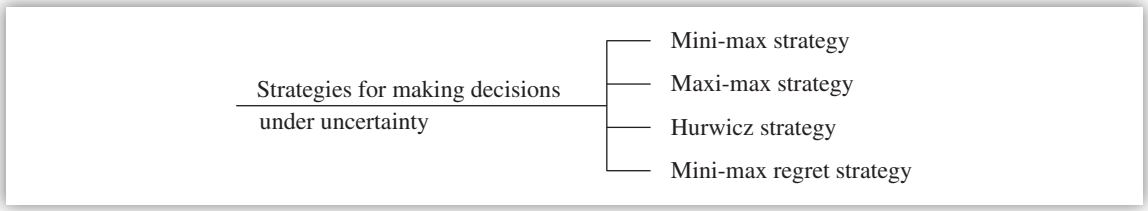


EXHIBIT 5.33 Strategies for Making Decisions under Uncertainty

The **mini-max strategy** is a very conservative, pessimistic strategy that assumes that whatever action we choose, nature is against us and will cause the worst possible outcome. The values of the worst outcomes are the row minima. This strategy calls for choosing the action that gives us the best (largest) of these minima. That is, it chooses the action whose worst possible outcomes are not as bad as the worst possible outcomes of the other actions.

The best examples of applications for uncertainty are in problems of the military, war, and various types of athletic competition, product development, product pricing, collective bargaining, arbitration, foreign policy decisions, contract bidding, and oligopolistic and monopolistic market conditions.

The mini-max strategy has the nice property that it guarantees an outcome that is no worse than the minimum value for the action. The outcome may be better than the minimum, but it will certainly be no worse. However, this strategy, which focuses on preventing disaster, has the unfortunate property that it may eliminate the best outcomes from consideration.

The **maxi-max strategy** is an optimistic strategy that assumes that nature will cooperate with us to provide the best possible outcome for the action we choose—the row maxima. This strategy chooses the action that yields the best of the possible outcomes. However, it does not defend the decision maker against the possibility of containing the worst possible outcome, as does the mini-max strategy. Decision makers who are attracted to large gains would most likely use the maxi-max decision rule.

APPROACHES TO DECISION PROBLEMS

Whatever strategy we decide to use in approaching decision problems, it is wise to make a habit of determining if any of the alternatives is dominating and could therefore be eliminated.

The **Hurwicz strategy** is a compromise between the very pessimistic mini-max strategy and the very optimistic maxi-max strategy. A value between 0 and 1 is chosen for the coefficient of optimism, A, keeping in mind that low values of A are an indication of pessimism and high values of A are an indication of optimism. The goal is to find both the row minima and the row maxima and choose the activity that yields the maximum of the computed quantities. When A is zero, the Hurwicz strategy is the same as the mini-max strategy; when A is 1, the Hurwicz strategy is the same as the maxi-max strategy.

MINI-MAX STRATEGY VERSUS MAXI-MAX STRATEGY

- The mini-max strategy is a pessimistic strategy and finds the *row minima*. It gives a conservative feel when playing a game against nature but not when playing against a human opponent. This is because we know our opponents.
- The maxi-max strategy is an optimistic strategy and finds the *row maxima*.

The **mini-max regret strategy** is good for situations where the expected values concept fails. Why does the expected value technique fail? Expected values are averages of values. They are appropriate when we are trying to balance values that are close together, for example, the chance of losing $2.00 versus the chance of winning $4.00. Averages are much less appropriate when we balance values that are very different, such as the cost of a modest insurance premium versus the risk of being impoverished by a serious car accident.

The mini-max regret decision criteria choose the strategy that minimizes the maximum opportunity cost. To measure regret, take the difference between the value of the outcome actually obtained and the maximum value that could have been obtained if a different alternative had been chosen.

DECISIONS UNDER RISK VERSUS DECISIONS UNDER UNCERTAINTY

- Probabilities can be computed for decisions under risk.
- Probabilities cannot be computed for decisions under uncertainty.

Decision Making under Conflict Decision making under conflict is referred to as game theory. The mini-max strategy is used for analyzing decisions under conflict or competition. There are two types of games under conflict: zero-sum game and non-zero-sum game.

Game theory is used when the states of nature of the decision maker are the strategies of the opponent. When one opponent gains at the loss of the other, it is called a **zero-sum game** involving a complete conflict of interest. Games with less than complete conflict of interest are termed **non-zero-sum games**. In non-zero-sum games, the gains of one competitor are not completely at the expense of the other competitors.

The majority of business competitive actions involve non-zero-sum games. Non-zero-sum games require that the payoffs be given for each player since the payoff of one player can no longer be deducted from the payoff of the other, as in zero-sum games. **Prisoner's dilemma** is a type of business game situation where one firm is concerned about the actions of its rivals. The outcome of the prisoner's dilemma game cannot be predicted conclusively. An example of payoff table is shown in Exhibit 5.34.

States of Nature

	1	2	3	4	Expected profit
A					
B					
C					

EXHIBIT 5.34 Payoff Table

States of nature are uncontrollable future events that can affect the outcomes of a decision. The best examples of applications of zero-sum games are in problems of the military, war, and various types of athletic competition. The best examples of applications of non-zero-sum games are in product development, product pricing, collective bargaining, arbitration, foreign policy decisions, contract bidding, and oligopolistic and monopolistic market conditions.

The simplest type of gain is the two-person zero-sum game. The players, X and Y, are equal in intelligence and ability. The term "zero sum" is used because the sum of gains exactly equals the sum of losses. The sum of player X's gains (or losses) and player Y's losses (or gains) is zero. Such a game, in which the sum of gains and losses added up over all players is zero, is called a zero-sum game.

Example of Utility for Alternatives

Assume a linear utility for money and a risk-neutral decision maker. From the next payoff table, we can conclude that the utility for alternative A is

	State of Nature		
	S1	**S2**	**Expected Profit**
Alternative A	100	200	$160
Alternative B	140	40	$ 80

a. $300.

b. High.

c. Exactly twice that of B.

d. Approximately twice that of B.

The correct answer is **c**. The utility function for money would be linear, and the decision maker's behavior would be consistent with the maximization of expected profit. A risk-neutral decision maker will select the alternative with the highest profit, that is, alternative A, which is exactly twice that of B (160/80 = 2). Choice (a) is incorrect. Utility is measured in "utils, not in dollars." It does not compare the two alternatives. Choice (b) is incorrect. This requires a judgment about the utility function of the decision maker, which is unknown. Choice (d) is incorrect. The linearity assumption leads to exact statements, not approximations.

(E) Pure Strategy and Mixed Strategy A pure strategy exists if there is one strategy for player X and one strategy for player Y that will be played each time. The payoff, which is obtained when each player pays the pure strategy, is called a **saddle point**. The saddle point represents an equilibrium condition that is optimum for both competitors.

The **Wald criterion,** which is a variant of decision making under uncertainty, is a useful technique to determine if a pure strategy exists. A saddle point can be recognized because it is both the smallest numerical value in its row and largest numerical value in its column. Not all two-person zero-sum games have a saddle point. When a saddle point is present, complex calculations to determine optimum strategies and game values are unnecessary.

When a pure strategy does not exist, a fundamental theorem of game theory states that the optimum can be found by using a mixed strategy. In a mixed strategy, each competitor randomly selects the strategy to employ according to a previously determined probability of usage for each strategy. Using a mixed strategy involves making a selection each time period by tossing a coin, selecting a number from a table of random numbers, or using some probabilistic process.

There is a simple test to determine whether a pure or mixed strategy is best. If the maximum of the row minima (the maxi-min) equals the minimum of the column maxima (the mini-max), then a pure strategy is best. Otherwise, use the mixed strategy.

KEY CONCEPTS TO REMEMBER: Which Decision Criterion Is What?

Mini-max criteria	→	Minimizing the maximum losses
Maxi-max criteria	→	Maximizing the maximum profits
Maxi-min criteria	→	Maximizing the minimum profits
Mini-min criteria	→	Minimizing the minimum losses or maximum profits (not worth pursuing)
Mini-max regret criteria	→	Minimizing the maximum opportunity cost

(F) Decision Making versus Problem Solving Decision making and problem solving are not the same; they have two different time dimensions. The basic difference is that decision making is future oriented and problem solving is past oriented. Decision making deals with risk while problem solving does not.

Decision making is the probability of success. Examples of decision-making situations include investing in a new product line, buying new equipment, and selecting an employee for a key position. Examples of problem-solving situations include handling a tardy employee, correcting a poor-quality production, and working with a slow-paying customer.

Exhibit 5.35 presents an overview of differences between decision making and problem solving.

Decision making	Problem solving
Decision making is concerned with future consequences; it changes the environment and the situation.	Problem solving is concerned with looking back; this is the way it should be and it no longer is.
A decision is made to create a change and therefore generates a new set of circumstances.	A problem is solved now so that decision making is not needed later. This is because the problem-solving approach has restored the process where it should be.
Decision making focuses on making things happen in the future.	Problem solving can be greatly overdone because it creates a fear of change.
A decision has a risk and an uncertainty, but it also creates an opportunity.	A change should be seen as an opportunity to go forward, not to go back to the past.

EXHIBIT 5.35 Differences between Decision Making and Problem Solving

Source: Peter F. Drucker, *The Frontiers of Management* (New York: Harper & Row; 1986).

(G) Decision Making and the Internal Auditor: Applications In order for auditors to reach decisions, they must understand how the various pieces of information are combined. For example, the issues of materiality, conflicting evidence, and determining whether sufficient evidence has been gathered all influence the auditor's decision-making process.

The internal auditor will be making decisions under various circumstances. When the auditor must make an important decision in a hurry and that decision is based on incomplete information, the decision-making process would be called satisficing, not maximizing, minimizing, or rationalizing. "Satisficing" is a nonoptimization decision-making method. The auditor presents several audit situations that require a decision.

- **Audit Situation No. 1.** The director of internal auditing of a manufacturing company is updating the long-range audit schedule. Several possible audit assignments can fill a given time spot. Information on potential dollar exposure and key internal controls has been gathered. The director has four choices to choose from, based on perceived audit risks, and needs to select the assignment of greatest merit. The four choices are:

  1. Precious metals inventory—book value, $1,000,000; separately stored but access not restricted.
  2. Branch office petty cash—ledger amount, $50,000; 10 branch offices, equal amounts; replenishment of accounts requires three separate approvals

3. Sales force travel expenses—budget, $1,000,000; 50 salespeople; all expenditures over $25 must be receipted.
4. Expendable tools inventory—book value, $500,000; issued by tool crib attendant upon receipt of authorization form.

The audit director will select the choice 1 because of its relatively high risk. Precious metals include gold and silver, which are subject to theft or loss. Also, the access is not restricted. Choice 2 is not a high-risk situation because replenishment of petty cash requires three separate approvals and the total dollar amount is less than choice 1. Choice 3 is not a high-risk situation since all expenditures over $25 must be receipted. Choice 4 is not a high-risk situation because upon receipt of an authorization form, the tool crib attendant issues expendable tools. Key internal controls are adequate in situations described by choices 2, 3, and 4. Controls are inadequate in choice 1.

- **Audit Situation No. 2.** An internal auditor is planning an audit of the personnel department of her company. She needs to make a decision about audit objectives. The appropriate audit objective would be to determine if reference checks of prospective employees are being performed. It would not determine whether: hourly employees are being paid only for hours actually worked as indicated by time cards or similar reports; an equitable training program exists that provides all employees with approximately the same amount of training each year; or recruitment is being delegated to the various departments that have personnel needs.
- **Audit Situation No. 3.** During an audit of the HR department, an internal auditor plans to evaluate controls over the termination process. If audit work steps are to be prioritized, the auditor should do this audit step first: Evaluate procedures used to communicate termination actions to the payroll department. The auditor should not first examine employee turnover rates for the most recent years, reasons for termination as shown in exit interviews, or costs associated with replacing terminated employees.
- **Audit Situation No. 4.** An internal auditing team has identified findings that should significantly improve a division's operating efficiency. In appreciation for this fact, and because it is the Christmas season, the division manager presents the in-charge auditor with a gift that has a value of approximately $100. The auditor needs to make a decision between his personal ethics and the IIA's Code of Ethics. The correct decision is that he should not accept the gift without the knowledge and consent of the director of internal auditing and that he should not accept it, regardless of other circumstances, because its value is significant.
- **Audit Situation No. 5.** An internal auditor is involved in a fraud investigation. She needs to make a decision about the most appropriate audit activity that she should undertake. The correct approach is to design procedures to follow in attempting to identify the perpetrators and causes of the fraud. She should not supervise the activities of security personnel and other investigators, serve as liaison with law enforcement personnel and the press, or conduct public interrogations of suspected perpetrators.
- **Audit Situation No. 6.** An internal auditor is examining accounts receivable balances. He needs to make a decision to obtain the most competent type of evidence. He should receive positive confirmations directly from the customers. The least competent evidence would be when he interviews the personnel who records accounts receivable, verifies that postings to the receivable account from journals have been made, and assures himself that no response has been received for a request for a negative confirmation.

- **Audit Situation No. 7.** An internal auditor is preparing working papers in connection with plant maintenance costs audit. She needs to differentiate between necessary and unnecessary features of preparing a working paper. It is unnecessary to prepare a schedule of total acquisition cost of property, plant, and equipment for the preceding month. It is necessary to prepare a schedule showing total repair expense for the month preceding the audit.
- **Audit Situation No. 8.** An audit objective is to verify that the correct goods or services are received on time, at the right price, and in the right quantity. Based on this objective, an internal auditor needs to decide whether to audit the receiving department, the purchasing department, the manufacturing department, or the payroll department. The correct decision is to audit the purchasing department because it is the objective of that department to procure goods or services with all those attributes present (i.e., price, delivery, quantity, and quality).
- **Audit Situation No. 9.** A company makes a practice of investing excess short-term cash in marketable securities. An internal auditor is faced with a decision to select a reliable audit test of the valuation of those securities. The correct approach is to compare cost data with current market quotations. The following audit tests would not provide reliable tests for the valuation of those securities: confirmation of securities held by the broker, recalculation of investment carrying value using the equity method, or calculation of premium or discount amortization.
- **Audit Situation No. 10.** An internal auditor is planning to obtain evidence to support the legal ownership of real property. The best audit procedure he could choose would be an examination of closing document, deeds, and ownership documents registered and on file at the county courthouse. The following audit procedures would not provide the best audit evidence: examination of corporate minutes and board resolutions with regard to approvals to acquire real property discussion with corporate legal counsel concerning the acquisition of a specific piece of property, and confirmation with the title company that handled the escrow account and disbursement of proceeds on the closing of the property.
- **Audit Situation No. 11.** An internal auditor is performing an audit of the receiving department to determine if only authorized purchases are being accepted. She needs to make a decision about the type of documents that should be examined. The correct approach is to examine a "blind" (no quantities shown) copy of the purchase order received directly from the purchasing department. She should not examine: a bill of lading that has been accepted directly by the receiving department, an invoice that has been sent by the supplier directly to accounts payable, or a note documenting a telephone conversation with a purchasing agent.
- **Audit Situation No. 12.** A preliminary survey of the purchasing function indicates that: department managers initiate purchase requests that must be approved by the plant superintendent; purchase orders are typed by the purchasing department using prenumbered and controlled forms; buyers regularly update the official vendor listing as new sources of supply become known; rush orders can be placed with a vendor by telephone but must be followed by a written purchase order before delivery can be accepted; and vendor invoice payment requests must be accompanied by a purchase order and receiving report.

  An internal auditor is faced with a situation to decide what is relevant and what is irrelevant information with respect to controls, and he needs to identify one possible fault of this system. A risk exists that purchases could be made from a vendor controlled by a buyer at prices higher than normal.

- **Audit Situation No. 13.** An internal auditor is verifying a company's ownership of equipment. She needs to decide a course of action that would provide her the best evidence of ownership. She should choose to verify a canceled check written to acquire the equipment. Actions that would not provide the best evidence of ownership include: reviewing the current year's depreciation expense journal entry, conducting an interview with the equipment custodian verifying company ownership, or checking the presence of the equipment on the company's balance sheet.
- **Audit Situation No. 14.** The auditor is reviewing insurance coverage. His objective is to determine whether specified insurance coverage is being obtained economically. He needs to decide which audit procedure would be most appropriate to accomplish his objective. He would determine whether competitive bids were obtained from qualified insurance agents. He would not: inspect the insurance policies currently in force to determine compliance with company policies and the propriety of premiums; compare current-year insurance costs with those of the preceding two years on a total and on a risk-by-risk basis; or interview the head of the insurance department to ascertain procedures employed in identifying risks, purchasing insurance, and obtaining dividends.
- **Audit Situation No. 15.** Bank teller supervisors might manipulate accounts using their privileged computer access codes. They could withdraw money for their own use and move money among accounts when depositors complain to the bank about errors. The auditor needs to decide which procedures would most likely detect this potential problem. She would review transactions on privileged access codes since they are high-risk codes. She would not: review transactions for employees' accounts, verify proof records for teller access codes, or test the accuracy of account posting programs. These three procedures are good procedures for a normal audit but not for the problem situation described.
- **Audit Situation No. 16.** During an audit of a construction contract, it was discovered that the contractor was being paid for each ton of dirt removed. The contract called for payment made on cubic yards removed. There is a problem of mismatching the units of measure (i.e., ton versus cubic yards). The auditor needs to decide which documents need to be reviewed to correct this error. He would compare invoices to purchase orders or contracts since they indicate what should be the correct unit of measure. The auditor would not: compare invoices to receiving reports, compare actual costs to budgeted costs, or check the mathematical accuracy of invoice amounts. These three steps would not provide the official proof of the correct unit of measure since they are after-the-fact documents. A contract is the first and official document from which purchase orders are written.
- **Audit Situation No. 17.** An auditor is reviewing payments, and her objective is to ascertain the existence of improper payments. The auditor needs to decide which documents to review to satisfy her audit objective. She would decide to review payment-voucher supporting documents for receiving reports, invoices, purchase orders and approval-to-pay initials. The idea is that these documents would reveal any improper payments since they are the ones required for proper payment. The auditor would not: ask the treasurer's office personnel about the existence of duplicate payments, observe payment procedures in the treasurer's office for conformance to policies and procedures manual specifications, or compare total payments by type this year with those of prior years. These three procedures do not provide sufficient evidence to reach a valid conclusion.
- **Audit Situation No. 18.** Senior management has asked the internal auditing staff to conduct an audit of manufacturing safety facilities using an audit program originally designed by government auditors for use in Occupational Safety and Health Act (OSHA) investigations.

The auditor can justify using this standardized program because one responsibility of the internal auditor is to review systems to ensure compliance with laws. Audit objectives not pertinent to this request would include the means of safeguarding assets, the reliability and integrity of financial and operating information, and activities in coordination with others.

- **Audit Situation No. 19.** A car rental agency has branch offices throughout the world. Each branch is organized into three separate departments: maintenance, operations, and accounting. The auditor needs to decide the objectives for an operational audit. The information that would be most useful for the auditor is the objectives of each department. An operational audit would be more meaningful when the audit objectives include the objectives of the area to be audited. The following information would not be useful: the most recent financial data for each department, activity reports showing rental information for the different branches, and a complete listing of the perpetual inventory for the branch to be audited.
- **Audit Situation No. 20.** An auditor wishes to test the efficiency of a company's use of labor resources. He needs to decide an audit objective that would lead him to a test of the efficiency of labor resources. The audit objective would be to determine that employees are assigned to work situations equivalent to their training and skill level. The following audit objectives would not be relevant for the auditor's decision making: determining that all employees are paid in accordance with union wages (may be useful in a payroll audit), determining that the quality of performance by labor meets company standards, or determining that only authorized employees are paid (may be useful in a payroll audit).
- **Audit Situation No. 21.** An auditor needs to decide an audit procedure that best meets the objectives of determining that all sales are recorded. The appropriate audit procedure would be to test company controls that are designed to capture initial sales transactions as they occur. The following audit procedures would not achieve the desired objective: tracing sales invoices to subsidiary accounts receivable records, comparing current recorded sales totals with prior period, or vouching recorded sales from sales invoices to shipping documents.
- **Audit Situation No. 22.** An auditor noted that the accounts receivable department is separate from other accounting activities. Credit is approved by a separate credit department. Control accounts and subsidiary ledgers are balanced monthly. Similarly, accounts are aged monthly. The accounts receivable manager writes off delinquent accounts after one year, or sooner if a bankruptcy or other unusual circumstances are involved. Credit memoranda are prenumbered and must correlate with receiving reports. The auditor needs to decide which of the following areas could be viewed as an internal control weakness: write-offs of delinquent accounts, credit approvals, monthly aging of receivables, or handling of credit memos. Write-offs of delinquent accounts are a control weakness because the manager is not trying other avenues of collecting receivables prior to writing them off. The problem is that the manager is writing off delinquent accounts too soon.
- **Audit Situation No. 23.** Management wishes to include in its internal controls over factory payroll a procedure to ensure that employees are paid only for work actually performed. The auditor needs to decide an internal control action that would be most appropriate to achieve management's objective. She would compare piecework records with inventory additions from production since this provides her an objective basis for calculating the payroll. The following control actions would not achieve the objective: have foremen distribute paychecks to employees in their sections, use time cards, or keep unused paychecks in a vault. These three actions do not measure the work performed.

- **Audit Situation No. 24.** While performing an audit of cash, an auditor begins to suspect check kiting. The auditor needs to decide the best type of evidence that he can get concerning whether kiting is taking place. He would accomplish this by preparing a schedule of interbank transfers. "Kiting" is a term used for a scheme in which a depositor with accounts in two or more banks takes advantage of the time required for checks to clear in order to obtain unauthorized credit. Therefore, a schedule of interbank transfers would detect check kiting. The following evidence would not be useful: documentary evidence obtained by vouching entries in the cash account to supporting documents, documentary evidence obtained by vouching credits on the latest bank statements to supporting documents, or oral evidence obtained by discussion with controller personnel.
- **Audit Situation No. 25.** An auditor wishes to estimate inventory shrinkage by weighing a sample of inventory items. From past experience, she knows that few specific items are subject to unusually large amounts of shrinkage. The auditor wants to decide the best course of action using statistical sampling. She should stratify the inventory population so those items subject to unusually large amounts of shrinkage are reviewed separately. The following courses of action would not be useful: eliminating any of the items known to be subject to unusually large amounts of shrinkage, increasing the sample size to lessen the effect of the items subject to unusually large amount of shrinkage, or continuing to draw new samples until a sample is drawn that includes none of the items known to be subject to large amounts of shrinkage.
- **Audit Situation No. 26.** An auditor is planning an audit program for her company's purchasing department. The auditor discovered four situations related to purchasing activities.

  1. User departments, instead of purchasing, are selecting suppliers and ordering goods.
  2. The make-or-buy committee does not have a written set of procedures.
  3. Quantitative and qualitative yardsticks on purchasing activities are absent.
  4. Rotation of buyer assignments is not accomplished.

  The audit objective is to determine if goods and services are obtained at the best price. The auditor needs to make a decision how best to allocate audit resources to the four purchasing activities. A risk ranking approach would be useful here. She would review activity 1 first, activity 4 next, activity 3 next, and activity 2 last, because activity 1 is a high risk and activity 2 is a low risk.
- **Audit Situation No. 27.** In an audit of a purchasing and payables system, the auditor has determined that invoices are sometimes paid twice, goods are paid for that were never received, materials have been shipped to an assistant buyer's home, and invoices for goods returned to vendors are sometimes paid—quite a few serious problems! The auditor's objective is to obtain sufficient evidence for each one of these problems.
  - A random sample found 10 paid vouchers without an accompanying original invoice. All 10 had been paid twice. This form of evidence would be both competent and sufficient in determining that invoices are paid twice.
  - A receiving report signed by the assistant buyer would be the strongest indicator that company-paid materials have been shipped to an assistant buyer's home.
  - An examination and accounting of shipping documents prepared for all returns would provide sufficient evidence to support a conclusion that invoices are sometimes paid even though goods are returned to vendors.

- **Audit Situation No. 28.** An auditor wishes to test the effectiveness of data processing access controls. He needs to decide the audit procedure that would assist him in satisfying the audit objective. He would review access logs since they capture all accesses whether successful or not. He would not: study various access control software costs (may be appropriate in a software acquisition audit), analyze object code controlling access, or process test data simulating exception conditions. These three procedures do not achieve the audit objective at hand.
- **Audit Situation No. 29.** An auditor is verifying the existence of newly acquired fixed assets recorded in the accounting records. She needs to decide the best evidence to help achieve this objective. She would conduct a physical examination of a sample of newly recorded fixed assets to provide direct, firsthand evidence. The following items do not provide direct evidence: documentary support obtained by vouching entries to subsidiary records and invoices, oral evidence obtained by discussion with operating management, or documentary support obtained by reviewing titles and tax returns.
- **Audit Situation No. 30.** An auditor must make a decision about a test to determine whether purchase orders are being processed on a timely basis. The appropriate test would be to compare dates of selected purchase orders with those of purchase requisitions. Elapsed times can be measured with this test. The following tests would not be appropriate: determining the dates of unpaid accounts payable invoices, selecting a block of used purchase order numbers and account for all numbers in the block, or discussing processing procedures with operating personnel and observing actual processing of purchases. These three tests do not measure the elapsed time.
- **Audit Situation No. 31.** An auditor might use several different procedures to test for the proper accounting for retirement of plant and equipment. She needs to make a decision about a test that would be the most effective in providing evidence of retiring fixed assets. She would do analysis of debits to the accumulated depreciation account since this entry is done to retire fixed assets. The following tests would not be effective in achieving the stated objective: analysis of debits to the fixed-asset account (which is used to add new fixed assets), determination of whether fully depreciated assets still in use are included in the asset accounts, or examination of the cash account for unusual entries (assets may be retired without receiving any cash).
- **Audit Situation No. 32.** An auditor is evaluating the reasonableness of advertising expense. He needs to select the audit procedure providing the best evidence to achieve his objective. Analytical evidence developed by comparing the ratio of advertising expenses to sales with historical data for the company and industry would provide the auditor with the best evidence to meet his objectives. The following procedures would not provide the best evidence: oral evidence obtained through discussions with company marketing executives and representatives of the advertising agency retained, documentary evidence obtained by vouching charges to the account and by retracing charges from source documents to the account, or arithmetical evidence developed by recomputing charges submitted by the advertising agency and paid by the company.
- **Audit Situation No. 33.** The internal auditor in a consumer-products company plans to review marketing activities. She needs to decide actions that would contribute the most to determining whether the product-planning-and-development group has executed its responsibilities effectively. She would evaluate the acceptance of the company's products in the market by comparison with those of competitors. She would not: evaluate the organizational status of the group and its organizational structure; evaluate the coordination

between the group and other interested parties such as sales, finance, market research, and production; or evaluate the qualifications of personnel working in the group in relation to their specific assignments.

- **Audit Situation No. 34.** A logical substantive test for accrued interest receivable would be to recalculate interest earned and compare it to the amounts received. The following tests would not be logical: comparing the interest income with published interest-investment records; verifying the interest income by a calculation based on the face amount of notes and the nominal interest rate; or verifying the cost, carrying value, and market value of notes receivable. These three tests do not recalculate interest earned for checking its accuracy and do not compare to the amounts received, which is the focus of the substantive test.
- **Audit Situation No. 35.** An auditor is in the process of verifying the correct sales date for an item sold FOB shipping point. He needs to select the source document that would help him achieve his objective. He should select the carrier's bill of lading, not the customer's payment document, purchase order, or sales invoice. The bill of lading will indicate the correct shipping date at which the risk and ownership were transferred to the buyer. The other documents may or may not show the shipping date, let alone its accuracy.
- **Audit Situation No. 36.** While auditing a new computer system, the auditor discovered the design team had not complied with the company's system-development standards. What should the auditor do? She should expand test procedures as warranted by the deficiencies noted. She should not: instruct the design team to remedy the development deficiencies before reauditing the system, report the deficiencies to the external auditors, or terminate the audit.
- **Audit Situation No. 37.** A plant maintenance shop is experiencing excessive overtime. An auditor is planning to establish an appropriate objective for the audit. The objective should be to determine whether minimizing overtime requires a combination of preventive and corrective controls. The following would not be appropriate: developing work schedules based on the availability of skilled labor force; writing work order instructions in clear, understandable language; or delivering appropriate quantities of materials to work sites to meet work schedules.
- **Audit Situation No. 38.** A Certified Internal Auditor was found to be violating the IIA Code of Ethics. He should be anticipating the following action by the IIA board of directors: He should expect to forfeit the Certified Internal Auditor designation. He should not expect the following to happen: be discharged by his employer, pay a fine in the appropriate court, or receive an official reprimand.

5.2 Organizational Behavior

Topics such as organizational theory, organizational behavior, group dynamics, HR processes, and leadership skills are discussed in this section.

(a) Organizational Theory

(i) Theories of Organization

Basically two theories exist: the traditional view and the modern view. The traditional view has closed-system thinking while the modern view incorporates open-system thinking (see Exhibit 5.36).

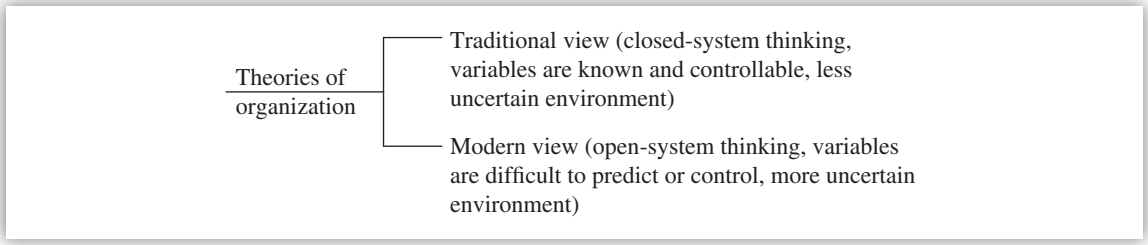


EXHIBIT 5.36 Theories of Organization

The **traditional view** assumes that the surrounding environment is fairly predictable and that uncertainty within the organization can be eliminated through proper planning and strict control. The primary goal is economic efficiency. All goal-directed variables are known and controllable.

The **modern view** assumes that both the organization and its surrounding environments are filled with variables that are difficult to predict or control. The organization interacts continuously with an uncertain environment. The primary goal is survival in an environment of uncertainty and surprise. The modern view deals with more variables that cannot be controlled or predicted.

Next we explore the evolution of traditional organization theory and its challenges followed by system characteristics.

(A) Traditional View of Organizations Henri Fayol and Frederick Taylor treated organizing as a subfield of management. They believed that close supervision, obedience, orders, and rules were the norm. Four traditional principles of organization emerged:

1. A well-defined hierarchy of authority (to ensure the coordinated pursuit of organizational goals)
2. Unity of command (each individual answered to only one superior)
3. Authority equal to responsibility (Authority is the right to get subordinates to accomplish objectives, and responsibility is the obligation to accomplish those objectives. Individuals should be accountable for getting something done only when they were given formal authority to get it done.)
4. Downward delegation of authority but not of responsibility (The obligation for getting something done remains with the superior although the authority and responsibility were passed along to subordinates.)

Later Max Weber called bureaucracy efficient because of the following four characteristics: (1) division of labor, (2) hierarchy of authority, (3) a framework of rules, and (4) impersonality (hiring and promoting people on the basis of what they know, not who they know). Bureaucracy is a matter of degree, and a moderate degree of bureaucratization can enhance organizational efficiency while extreme cases can hinder efficiency. However, trying to eliminate bureaucracy is impractical.

The traditionalists' rigid recommendations for organizing and managing were challenged since they did not work in all situations. Experience has proved that organizing was more than just strict obedience to authority and that bureaucracy has become the epitome of inefficiency. In addition, bottom-up authority and environmental complexity and uncertainty also challenged the traditional thinking about organizations.

Authority Is authority top-down or bottom-up? Traditionalists believed that authority was tied to property ownership and therefore naturally flowed from the top of the organization to the bottom. Chester Barnard questioned the traditional assumption about the automatic downward flow of authority. Instead, he proposed a more democratic *acceptance theory of authority* in which a leader's authority is determined by subordinates' willingness to comply with it.

Acceptance Theory of Authority

The acceptance theory of authority opened the door for upward communication and the informal organization that is based on friendship rather than work rules. Subordinates are viewed as active controllers of authority, not mere passive recipients.

Barnard believes that a subordinate recognizes a communication from a superior as being authoritative and decides to comply with it only when

1. The message is understood,
2. The subordinate believes it is consistent with the organization's purpose,
3. It serves the subordinate's interest, and
4. The subordinate is able to comply.

Uncertainty Charles Perrow observed that the increasing complexity of markets, variability of products, increasing number of branch plants, and changes in technology all required more adaptive organizations, not rigid structure. Plans usually have to be made on the basis of incomplete or imperfect information and, consequently, things do not always work out according to plan.

(B) Modern View of Organizations Proponents of open-systems views realize that system-to-system interactions are often as important as the systems themselves. Here the "system" includes social, political, legal, and economic systems. A highly organized and vigorously interactive world needs realistically dynamic models, which is a characteristic of open-system thinking.

CLOSED SYSTEMS VERSUS OPEN SYSTEMS

- Traditional closed-system thinking emphasizes rigid organization structure. It largely ignores environmental influences. Closed-system thinking does not have permeable boundaries. It assumes that all organizations are systems with common characteristics.
- Modern open-system thinking emphasizes the need for flexibility and adaptability in organization structure. It fosters a more realistic view of the interaction between an organization and its environment. Open systems have permeable boundaries. All organizations are open systems.

Four characteristics that emphasize the adaptive and dynamic nature of all modern open systems are (1) interaction with the environment, (2) synergy, (3) dynamic equilibrium, and (4) equifinality (see Exhibit 5.37).

Since open systems are not self-sufficient, they depend on the environment for survival (i.e., **interaction with the environment**). An open system adds up to more than the sum of its parts (i.e., **synergy**). A successful business is more than the factors of production: labor, land, and capital.

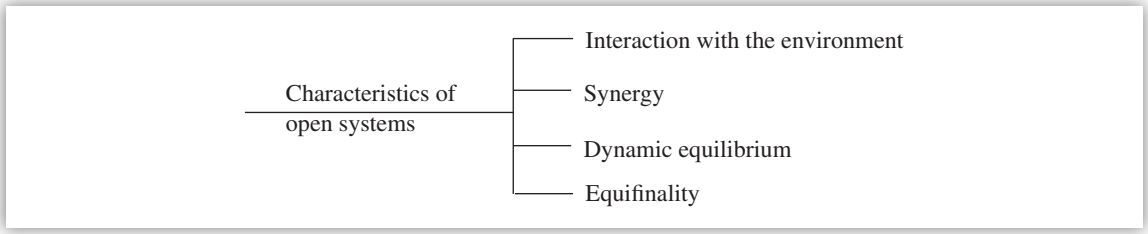


EXHIBIT 5.37 Characteristics of Open Systems

In open systems, dynamic equilibrium is the process of maintaining the internal balance necessary for survival by importing needed resources from the environment (i.e., **dynamic equilibrium**). **Equifinality** means reaching the same result by different means. It indicates that there is more than one way to get the job done.

Another way of looking at the open systems is in relation to subsystems. If a system is made up of subsystems, *three organizational subsystems would include technical, boundary spanning, and managerial*. The technical subsystem (production function) physically transforms raw materials into finished goods and services. Boundary-spanning subsystems facilitate the organization's interaction with its general environment. Most boundary-spanning jobs (interface functions) are easily identified by their titles. The managerial subsystem controls and directs the other subsystems in the organization.

KEY CONCEPTS TO REMEMBER: Open Systems

- Technical subsystems are the very core of the organization.
- Boundary-spanning subsystems are directed outward toward the general environment.
- The managerial subsystem serves as a bridge between the other two subsystems.

Many traditional theories of organizing exist, including bureaucracy, administrative theory, scientific management theory, and human relations theory. The latter topic is discussed briefly.

(ii) Human Relations Theory

Many management philosophers rejected the individualism, which was emphasized in the theories of bureaucracy, administrative theory, and scientific management. These new philosophers deplored competition between individuals in the organization and supported the idea of a cooperative group ethic. Emphasis was placed on the relations between people who are members of groups.

Mary Parker Follett and George Elton Mayo were two prominent philosophers associated with the **human relations movement**. Mary Parker Follett proposed the idea that individual freedom must be subordinated to the interest of the group. She was concerned with the individual but thought that the individual finds his or her creative self only by relating to others in groups. Follett thought that all authority rested on the consent of those who are directed. Therefore, she proposed that demands should arise from the situation rather than from the superior. Follett proposed that superiors should give reasons for their orders to subordinates. Participative management style is most likely to produce subordinates with management skills.

George Elton Mayo was very concerned with groups in the organization. He attempted to employ scientific methods to study the behavior of groups. He is most famous for his experiments at the Hawthorne Electric Plant in 1928, which in part investigated the influence of the degree of illumination on the productivity of workers. According to the Hawthorne studies, worker behavior is a complex system of forces that include personalities of the workers, nature of their jobs, and formal measurement and reward practices of the organization.

Closely related to the human relations movement is the **behavioral science** approach. Both of these approaches deal with the individual and his interaction in groups. However, the behavioral science approach arose because of the discontent with the methodology of researchers such as Mayo. Behavioral scientists deplored the small amount of data gathered by human relations advocates and the unsystematic examination of the data gathered.

Also, behavioral scientists thought that human relations writers overemphasized group behavior at the expense of individual behavior. Finally, behaviorists rejected the overriding concern with cooperation, when conflict may result in such benefits as innovation. It is easy to see that behavioral scientists emphasize the scientific method in investigating the individual and groups so that conclusions can be objective.

Behavioral scientists use three primary methods to study individuals and groups so that management can learn better ways of handling people. These methods are the case study, the sample survey, and the experiment. These three methods are inductive approaches since they involve studying a small number of persons or one organization and generalizing the results to other persons and organizations.

There are two primary criticisms of the behavioral science approach. First, it is not as precise a science as physics or chemistry because people are not as predictable as the nature of the universe. Second, behavioral science conclusions are useful, but since people and the environment in each organization are different, the application of findings may produce different results in different settings.

Douglas McGregor outlined a set of highly optimistic assumptions about human nature. He recommended Theory Y, which is a set of assumptions for his optimistic perspective about people. This is in contrast with the traditional view of people by managers (Theory X). He criticized Theory X for being pessimistic, stifling, and outdated. Exhibit 5.38 shows the comparison between Theory X and Theory *Y* assumptions about people from the manager's perspective.

Theory X assumptions	Theory Y assumptions
Most people are lazy, dislike or avoid work.	Work is a natural activity, and people are creative, energetic, and imaginative.
Most people must be coerced and threatened, and are unwilling to take responsibility.	The average person is willing to take responsibility.
Most people prefer to be directed.	People are capable of self-direction and self-control.
Most people are interested only in job security.	People are committed to do a good job if they are rewarded adequately.

EXHIBIT 5.38 McGregor Theory X/Y Assumptions

Senior management believes employees will volunteer to serve on committees because they: (1) want to play a greater role in the operation of their company, (2) want to receive more from their jobs than just a paycheck, and (3) have interests that extend beyond the boundaries of their specific jobs and will welcome the opportunity to pursue those interests. The motivational strategy that management has adopted is McGregor's Theory Y.

William Ouchi discovered a type of organization that exhibited a style of management that effectively combines the traits of typical American and Japanese companies. He called these hybrid companies **Theory Z organizations**. These companies focus on the employee in areas such as those listed next.

- Long-term employment
- Relatively slow evaluation and promotion
- Cross-functional career paths
- Participative decision making
- Individual responsibility
- Concern for employee
- Emphasis on employee self-control

Theory Z is an organizational culture based on a participative decision-making process.

Theory T and Theory T+ are complementary theories based on these Southeast Asian assumptions:

- Work is a necessity but not a goal itself.
- People should find their rightful place in peace and harmony with their environment.
- Absolute objectives exist only with God.
- In the world, persons in authority positions represent God, so their objectives should be followed.
- People behave as members of a family and/or group.
- Those who do not are rejected by society.

(iii) Contingency Design Theory

Organizing is the structuring of a coordinated system of authority relationships and task responsibilities. It spells out who does what and who reports to whom. Organizational structure can translate strategy into an ongoing productive operation (see Exhibit 5.39).

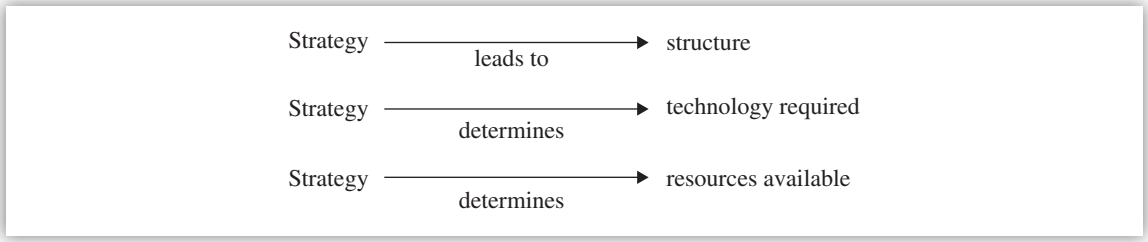


EXHIBIT 5.39 Strategy and Structure

Contingency design is an extension of the modern open-system view that permits the custom tailoring of organizations to meet unique external and internal situational demands. Contingency design is based on the assumption that there is no single best way to structure an organization. It is the process of determining the degree of environmental uncertainty and adapting the organization and its subunits to the situation. *Contingency design is fitting the organization's strategy to its internal and external environment.*

Two popular contingency models that validate the contingency approach by systematically matching structural characteristics with environmental demand include the Burns and Stalker model and the Lawrence and Lorsch model.

(A) Burns and Stalker model Behavioral scientists Tom Burns and G. M. Stalker proposed a typology for categorizing organizations by structural design. They distinguished between mechanistic and organic organizations (see Exhibit 5.40).

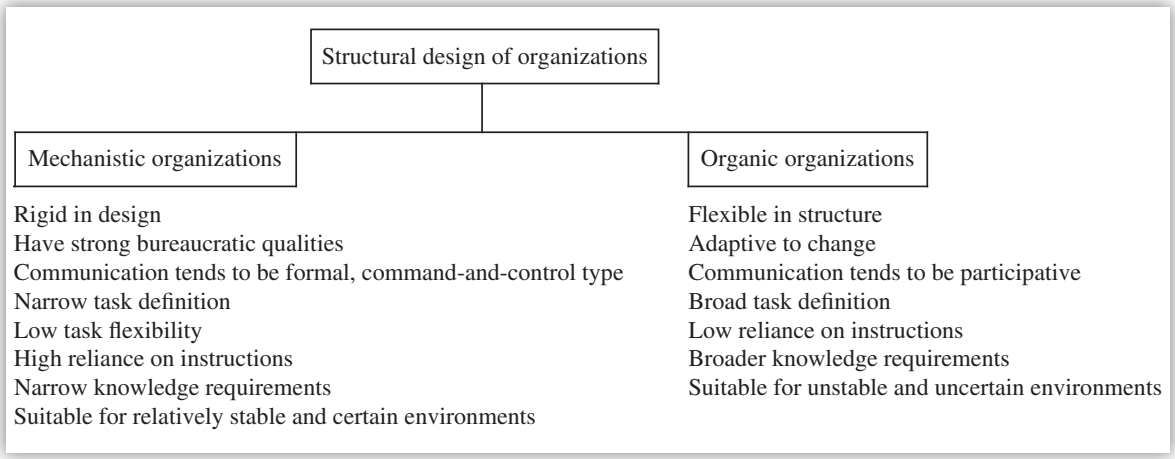


EXHIBIT 5.40 Structural Design of Organizations

(B) Lawrence and Lorsch Model Paul Lawrence and Jay Lorsch documented the relationships between two opposing structural forces (differentiation and integration) and environmental complexity. **Differentiation** resulting from a division of labor and technical specialization is the tendency among specialists to think and act in restricted ways. Differentiation tends to fragment and disperse the organization.

Integration, in opposition to differentiation, is the collaboration among specialists that is needed to achieve a common purpose. Integration is a unifying and coordinating force and is partially achieved through hierarchical control, standard policies and procedures, departmentalization, cross-functional teams and committees, better human relations, and liaison individuals and groups.

According to Lawrence and Lorsch, every organization requires an appropriate dynamic equilibrium (an open-system theme) between differentiation and integration. *They demonstrated that in successful firms, both differentiation and integration increased as environmental complexity increased.* These findings are equally applicable to the overall organization, departments, or divisions. They also found that the more differentiated an organization, the more difficult it is to achieve integration. These findings suggest that organizational failure in the face of environmental

complexity probably results from a combination of high differentiation and inadequate integration. Under these conditions, specialists work at cross-purposes and become involved in counterproductive conflicts.

Contingency design models conclude that there is no single best organization design and that the more uncertain the environment, the more flexible and adaptable the organization structure must be.

KEY CONCEPTS TO REMEMBER: Various Theories of Management

- Bureaucratic organization is characterized by division of labor, hierarchy (top-down) authority, a framework of rules, impersonality, formal policies and procedures, and a competency level for hiring and promotions. Bureaucracies focus on organizational tasks rather than people and emphasize productivity of human behavior and task results. Bureaucracies tend to be stable in the long run. Division of work deals with specialization of labor to achieve organizational objectives.
- The classical view of an early theory of management includes the universality concept. Esprit de corps, one of Fayol's 14 universal principles of management, emphasizes teamwork, communications, and harmonious effort among individuals. An example is "employees of a small retail outlet are highly motivated and genuinely concerned about the store's prosperity."
- The universal process is based on the belief that a single management process can be applied in all organizations. It believes that good managers are interchangeable among organizations. It uses a rigid, inflexible organizational structure regardless of the external environment.
- The operational approach, also known as scientific management or operations research, is concerned with technical, quantitative, and objective means of achieving efficiency in production operations. The manager is production oriented, and his or her primary interest is in improving efficiency and reducing waste. Standardization of work is a goal of the scientific school of management.
- Behavioral approaches to management primarily focus on people. They imply that it is in management's best interest to be concerned about employees' well-being. The behavioral approach to management most likely to resulted from the prospect of unionization.
- Operations management is a management process that designs, operates, and controls production systems. The focus of productive systems is to transform physical resources and human talent into needed goods and services. The operations management theory or approach views organizations as productive systems consisting of inputs, a transformation process, and outputs.
- In general systems theory, the term "subsystem" is used to describe the relationship of each system component to the next higher component. In the opinion of general systems theorists, all organizations are identified as being open. The systems approach to management views the organization as a system of interconnected and interdependent parts. It believes that the whole is greater than the sum of its parts. The systems approach to management is demonstrated by a chief executive officer (CEO) who stresses the importance of the interdependencies among the various components of the organization.
- Contingency management approach is practiced by a member who assigns responsibility and delegates authority based on the task to be performed and the individual available for assignment. Contingency management theory uses multivariate analysis to determine how a grouping of variables react together to produce an outcome.
- According to contemporary management thought, managers should be given training in a course linking key staffing issues with organizational strategy and structure. Such a course should include HR planning, selection, training, and performance appraisal.

- The principle of equity is concerned with fairness and justice.
- Under the scalar chain principle (chain of command), there is a chain of direct authority relationship from superior to subordinate. The scalar principle of management has been violated when an employee goes over the head of the supervisor and receives special permission from the departmental manager to, for example, take an extra week of vacation.
- The unity of command principle is violated when an employee answers to several bosses.
- Unity of direction requires the focus of all efforts aimed toward accomplishing the same goal, that is, in the same direction.

(b) Organizational Behavior

(i) Motivation Defined

The term "motivation" refers to the psychological process that gives a purpose and direction to human behavior. Motivation theories are generalizations about the "why" and "how" of purposeful behavior. The goal is to move individual employees toward achieving organizational objectives, including job performance. Kreitner[13] defines job performance as follows:

$$\text{Job performance} = \text{Ability} \times \text{Motivation}$$

Both ability and motivation are necessary for effective and efficient job performance. Ability and skills are acquired through education, training, and on-the-job experience. The individual's motivational factors—needs, satisfaction, expectations, and goals—are affected by challenging work, rewards, and participation. Motivational factors are both inborn and learned.

(ii) Motivation Theories

Four popular motivation theories exist: (1) Maslow's needs hierarchy theory, (2) Herzberg's two-factor theory, (3) expectancy theory, and (4) goal-setting theory (see Exhibit 5.41).

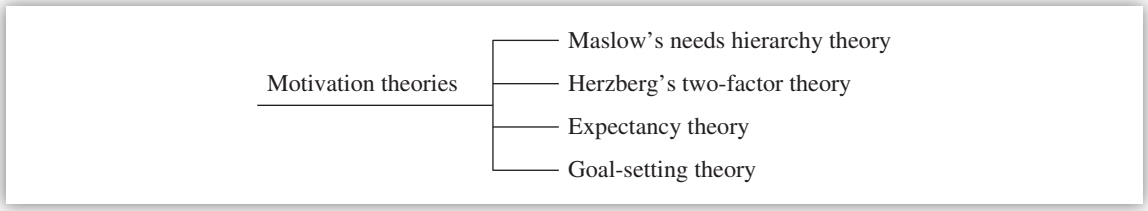


EXHIBIT 5.41 Motivation Theories

(A) Maslow's Needs Hierarchy Theory Maslow's theory focuses on five needs structured as a hierarchy, from bottom to top, and includes physiological, safety, love, esteem, and self-actualization needs. Individuals proceed up the hierarchy of needs, one level at a time. Higher needs emerge as lower needs are met. A fulfilled need does not motivate an individual. Needs are related to motivation in that unsatisfied needs motivate behavior. Maslow's esteem needs are most closely associated with Herzberg's concept of job enrichment.

[13] Kreitner, *Management.*

A major deficiency of Maslow's theory was "which higher-order needs come into play after the lower ones are satisfied and in which order they come into play cannot be predicted. If anything, it seems that most people are simultaneously motivated by several of the same-level needs." Another criticism is that individual perception is secondary. Maslow's needs theory failed under actual testing.

(B) Herzberg's Two-Factor Theory Herzberg's theory was based on employee satisfaction in that a satisfied worker is motivated from within to work harder and a dissatisfied employee is not self-motivated. Herzberg's two factors are satisfiers and dissatisfiers. Dissatisfaction is associated with complaints about the job context or factors in the immediate work environment. Exhibit 5.42 presents some factors labeled as satisfiers and dissatisfiers.

Dissatisfiers	Satisfiers
Company policy and administration	Achievement
Supervision	Recognition
Relationship with supervisor, peers, and subordinates	Work itself
Work conditions	Responsibility
Salary	Advancement
Personal life	Growth
Status	
Security	

EXHIBIT 5.42 Satisfiers versus Dissatisfiers

The elimination of dissatisfaction is not the same as truly motivating an employee. Herzberg is convinced that money is a weak motivational tool because, at best, it can only eliminate dissatisfaction. To satisfy and motivate employees, an additional element is required: meaningful, interesting, and challenging work. Critics argued that his theory was weak on an empirical basis, and the individual's perception was secondary. Others argued that one person's dissatisfier may be another's satisfier. Herzberg's biggest contribution is the motivating potential for enriched work.

(C) Expectancy Theory Individual perception, although secondary in the Maslow and Herzberg models, is central to expectancy theory. Expectancy theory is based on the assumption that motivational strength is determined by perceived probabilities of success. The term "expectancy" refers to the subjective probability (or expectation) that one thing will lead to another. The focus of this model is as follows: One's motivational strength increases as one's perceived effort–performance and performance–reward probabilities increase. This theory has received empirical support from researchers and is based on common sense since *Effort* → *Performance* → *Reward.* Employees tend to work harder when they believe they have a good chance of getting personally meaningful rewards.

(D) Goal-Setting Theory Goal setting is the process of improving individual or group job performance with clear objectives and high standards. Management by objectives (MBO) is an example of goal-setting theory.

Management by Objectives Organizational goals can be better achieved if the goals of superiors and subordinates are integrated with organizational goals. All levels of management should be involved in setting the objectives of the organization in working toward the common goals.

The essence of MBO is close consultation between superior and subordinate in the setting of and agreement on goals. They must agree on the goals to be achieved. Feedback is necessary during the period of working toward the goals and after the goals are accomplished. A key requirement is unity of command. Unity of command requires subordinates to be evaluated by a single superior—the manager.

MBO characteristics are listed next.

- Organizational common goals and measures of the achievement of the goals are complied.
- If necessary, the organizational structure is changed. That is, the chain of command and the unity of command may have to be changed.
- Each superior confers with each subordinate on the subject of the subordinate's goals.
- The superior and subordinate must agree on the subordinate's goals and the criteria for achieving the goals.
- The subordinate must be given feedback on achievement of the goals based on the criteria established.
- The performance of the subordinate must be reviewed.
- The performance of the organization must be reviewed periodically.
- When implementing MBO, these problems/barriers can be encountered:
  - Unity of command must be achieved.
  - Managers must change to a democratic style of leadership.
  - Accomplishment of goals that are nonquantifiable may be difficult to measure.

See Exhibit 5.43 for advantages and disadvantages of MBO.

Advantages of MBO	Disadvantages of MBO
Improves communications between superiors and subordinates	Opposition by managers for employee participation
Performance evaluation relatively easier due to established criteria	Suboptimization can occur
Room for innovation and creativity	Difficulty in reaching agreement on goals
Results in fewer or no surprises to managers	Learning is on trial-and-error basis
	Imposition of external factors (e.g., economy) on employee goals without full control over them

EXHIBIT 5.43 Advantages and Disadvantages of MBO

WHICH MOTIVATION THEORY IS WHICH?

- Maslow's theory is built around the hierarchy of human needs.
- Herzberg's theory is concerned with job performance and job satisfaction and focuses on maintenance and motivational factors.
- Expectancy theory is based on concept that people's expectations of rewards are derived from their unique personal motive structure, beliefs, and perceptions.
- Goal-setting theory (MBO) is based on improving individual or group job performance.

(iii) Motivation Strategies

Motivation strategies were derived from the motivational theories discussed previously. These strategies are listed next.

- Motivation through job design
- Motivation through rewards
- Motivation through employee participation
- Motivation through work schedules and services

(See Exhibit 5.44.)

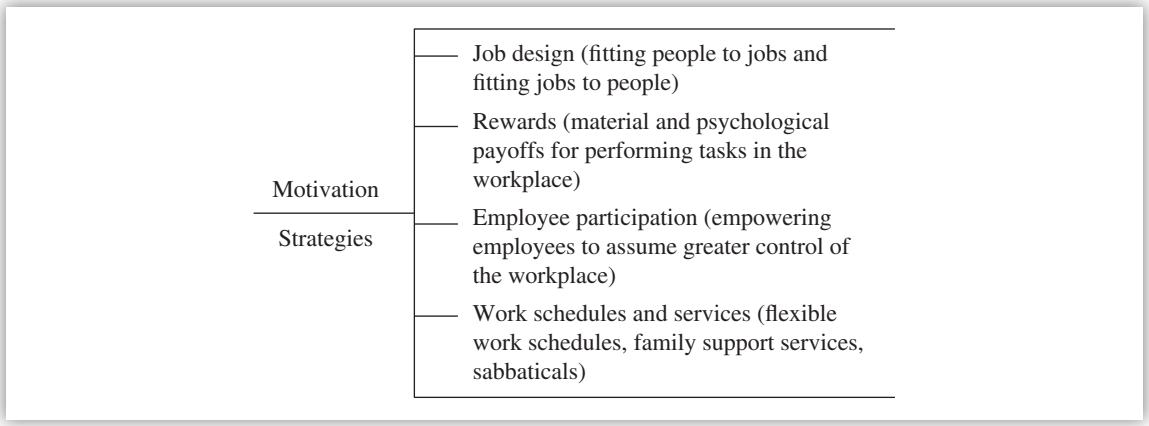


EXHIBIT 5.44 Motivation Strategies

(A) Motivation through Job Design Motivation through job design deals with two specific strategies: fitting people to jobs and fitting jobs to people. Three proven alternatives in fitting people to jobs include realistic job previews, job rotation, and limited exposure.

Job previews deal with audiovisual previews about the job and written descriptions in booklet form. Surveys have shown that those who were given realistic job previews tended to have lower initial expectations, greater organizational commitment and job satisfaction, and a lower turnover rate. However, the impact of realistic job previews on job performance was mixed.

Job rotation involves periodically moving people from one specialized job to another. It permits employees to rotate among several job positions. Job rotation provides for the continual development of managerial skills.

Limited exposure deals with limiting the individual's exposure to tedious and highly fragmented jobs. This technique is called "earned time off," which involves establishing a challenging yet fair daily performance standard and letting employees go home when the standard is reached.

The strategy of fitting jobs to people includes job enlargement and job enrichment. Job enlargement is the process of combining two or more specialized tasks in a work flow sequence into a single job. Job enrichment is redesigning a job to increase its motivating potential. It increases the challenge of work by reversing the trend toward greater specialization. Unlike job enlargement, which merely combines equally simple tasks, job enrichment builds more complexity and

depth into jobs by introducing planning, decision making, and responsibility normally carried out at higher levels. Job enrichment may motivate employees because it addresses the work itself instead of trying to change the workers to fit the jobs.

JOB ENRICHMENT VERSUS JOB ENLARGEMENT

- Job enrichment adds depth to a job.
- Job enlargement adds width to a job.

Exhibit 5.45 presents a comparison of characteristics between job enrichment and job enlargement.

Characteristics of job enrichment	Characteristics of job enlargement
Jobs are loaded vertically.	Jobs are loaded horizontally.
It allows employees to participate in planning and controlling.	It combines two or more specialized tasks but does not increase the planning or decision-making aspects of the job.
It promotes employee discretion and judgment.	
It gives a feeling of personal responsibility.	

EXHIBIT 5.45 Comparison of Job Enrichment and Job Enlargement

(B) Motivation through Rewards Every employee expects to be rewarded in some way for work performed. Rewards may include material and psychological payoffs for performing tasks in the workplace. Managers have found that job performance and satisfaction can be improved by properly administered rewards. Two types of rewards exist: (1) extrinsic rewards, which are payoffs granted to the individual by other people (e.g., money, employee benefits, promotions, recognition [employee of the month], status symbols, and praise) and (2) intrinsic rewards, which are self-granted and internally experienced payoffs (e.g., sense of accomplishment, self-esteem, and self-actualization). An intrinsic reward is an internally generated benefit or satisfaction resulting from good work performed (see Exhibit 5.46).

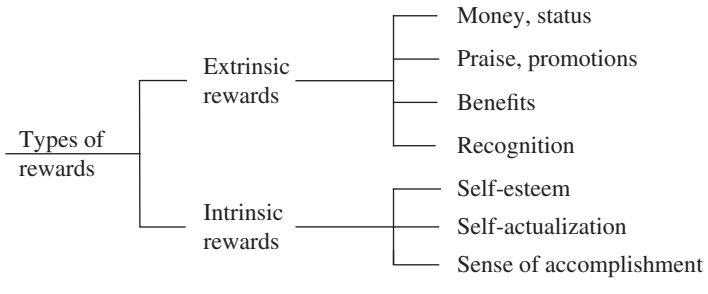


EXHIBIT 5.46 Types of Rewards

Example

A positive motivational effect will take place when a director of internal auditing decides to fill a supervisory vacancy by promoting a senior auditor rather than recruiting an outsider for the position.

(C) Motivation through Employee Participation "Participative management" is defined as the process of empowering employees to assume greater control of the workplace. Employees may participate in setting goals, making decisions, solving problems, and designing and implementing organizational changes. Employee participation will not work if individual values and attitudes are not in tune with it. Organizational factors, such as job design and corporate culture, can also help or hinder the process. Environmental factors, such as technological change and competition, also affect the participation process.

Two team-oriented approaches to employee participation include quality control circles and self-managed teams. *Quality control circles* are small groups of voluntary, problem-solving employees who meet regularly to discuss quality improvement and ways to reduce costs. To be successful, the quality control circles should be introduced in an evolutionary manner rather than by management order.

Self-managed teams (or autonomous work groups) take on traditional managerial tasks as part of their normal work routine. Advocates say self-managed teams foster creativity, motivation, and productivity. The manager's role will be more of a facilitator than an order giver, and supervision tends to be minimal. Hiring, training, and job design need to be skillfully interlocked with self-managed teams, thus driving up front-end costs. Traditional authoritarian supervisors view self-managed teams as a threat to their authority, job security, and power.

QUALITY CONTROL CIRCLE VERSUS SELF-MANAGED TEAMS

- Quality control circles foster employee participation within the confines of the existing power structure.
- Self-managed teams create a whole new decentralized power structure.

(D) Motivation through Work Schedules and Services Approaches such as flexible work schedules, family support services, and sabbaticals are aimed at enhancing employee motivation and increasing job performance. While employees liked flexible work schedules, employers did not like them because of greater administrative expense, supervisory resistance, and inadequate coverage of jobs. Alternative approaches were invented, such as compressed workweeks (40 hours in fewer than five days), permanent part-time jobs (workweeks with fewer than 40 hours), and job sharing (complementary scheduling that allows two or more part-timers to share a single full-time job).

(c) Group Dynamics

(i) How Groups Think and Make Decisions

(A) Overview Today, groups or committees make many decisions in organizations. There is a link between communication concepts and the subject of group decision making. Since messages are transmitted between members of the group, the effectiveness of this communication process will have a greater impact on the quality of the group's decisions.

Groups offer an excellent vehicle for performing many of the steps in the decision-making process.[14] They are a source of both breadth and depth of input for information gathering. If the

[14] Stephen P. Robins, *Organizational Behavior* (Englewood Cliffs, NJ: Prentice Hall, 1993).

group is composed of individuals with diverse backgrounds, the alternatives generated should be more extensive and the analysis more critical. When the final solution is agreed on, there are more people in a group decision to support and implement it. These pluses, however, can be more than offset by the minuses—time consumed by group decisions, the internal conflicts they create, and the pressures they generate toward conformity.

KEY CONCEPTS TO REMEMBER: The Group Decision—Strengths and Weaknesses

- **Strengths or assets.** Breadth of information, diversity of information, acceptance of solution, and legitimacy of process
- **Weaknesses or liabilities.** Time consuming, conformity, domination of discussion, ambiguous responsibility, and loss of personal accountability

(B) Group Behaviors Group psychology studies have revealed that various groups produced contradictory behavior. Sometimes people did better at their tasks when there were other people around and sometimes they did worse.

Groupthink, groupshift, and group polarization are the three by-products of group decision making, all of which have the potential to affect the group's ability to evaluate alternatives objectively and arrive at quality decision solutions (see Exhibit 5.47).

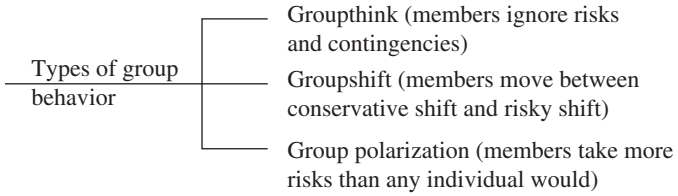


EXHIBIT 5.47 Types of Group Behavior

Groupthink is related to norms and describes situations in which group pressures for conformity deter the group from critically appraising unusual, minority, or unpopular views. Groupthink is a disease that attacks many groups and can dramatically hinder their performance. Individuals who hold a minority position that is different from that of the dominant majority are under pressure to suppress, withhold, or modify their true feelings and beliefs. Opposition is viewed as disloyal and is discouraged. Groupthink can ignore risks and contingencies. The group leader must remain impartial and play the devil's advocate to come up with new challenges and alternatives.

Groupshift indicates that in discussing a given set of alternatives and arriving at a solution, group members tend to exaggerate the initial position that they hold. Groups move between conservative shift and risky shift. The fact that it is a group decision frees any single member from accountability for the group's final choice. Greater risk can be taken because even if the decision fails, no one member can be held fully responsible.

Group polarization can occur when a group decides to take more risks than any individual would have judged reasonable. Groups tend to make more extreme decisions than individuals who are

part of the group. Group polarization and groupthink are two extremes on a risk measurement scale (see Exhibit 5.48).

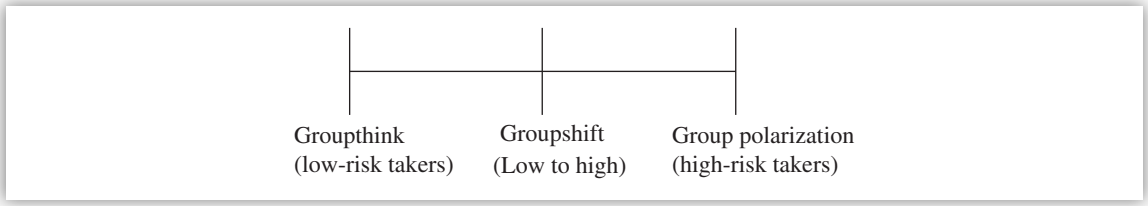


EXHIBIT 5.48 Groupthink and Group Polarization

(ii) Factors Affecting Group Decisions

Many factors affect group decisions, including ownership, nature, and structure of the problem; and nature, maturity level, size, and climate of the group (see Exhibit 5.49).

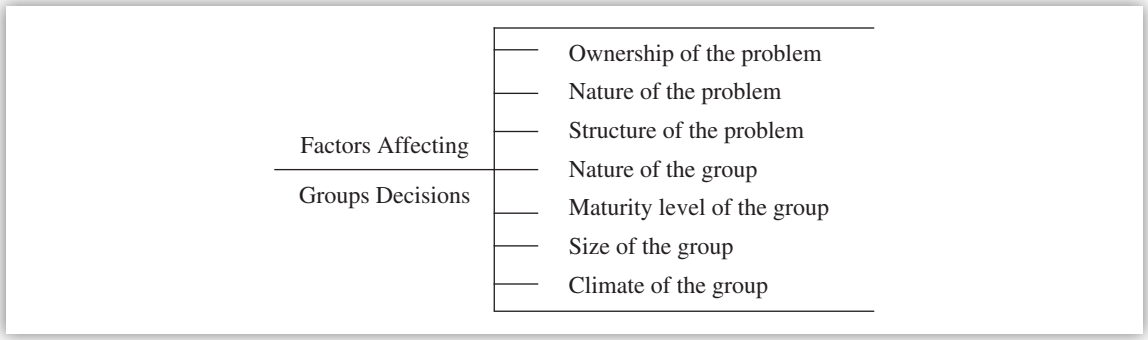


EXHIBIT 5.49 Factors Affecting Group Decisions

(A) Ownership of the Problem One of the selection criteria for a problem-solving method focuses on whether the problem is one that is "owned" by an individual or by a group. Individual ownership means that one person has the major interest in the solution of a problem; in effect, the group then works for that person. Group ownership means that several individuals or departments have an investment in the solution of a particular problem. Synectics is a good technique to use to solve problems owned either by individuals or by groups.

(B) Nature of the Problem Not all problems can or should be solved by a group of people. One or two people might straighten out a problem if they have enough information and if they can take actions to remedy the problem by themselves. But if the problem is uncertain—that is, if not enough is known about it or the strategies for achieving a solution, or if implementation of the solution requires the acceptance, investment, or action of many people—then the best approach is to work with a group.

(C) Structure of the Problem Another dimension to decision making is the structure of the problem. Structure has to do with the routineness of the decision required. How much is known or understood about the problem? If a problem is structured, if it is well understood, and if there are routine ways of dealing with it, the group can usually move quickly from the problem identification stages to the generation of solutions. But if a problem is unstructured or if it is not well understood, the group will need to spend a good deal of time identifying the problem before moving on to subsequent stages.

(D) Nature of the Group Basically, group membership should reflect the level of the problem. For example, if the problem is a departmental one, then members of the department should be asked to resolve it. Participants should also be considered with regard to their potential functions within the group. Ideally, the membership should include people who are knowledgeable about various aspects of the problem: technical, political, organizational, environmental, personal, and so on. In addition, since any final solution needs to be accepted by those who will implement it, the people who actually will carry out the solution should be present in the group. The presence of knowledgeable people improves the quality of the decision; implementers improve the acceptance of it.

(E) Maturity Level of the Group Knowledge of the maturity of the group helps to gain a clear understanding of its dynamics. "Group maturity" refers to the length of time a group has worked together and the kinds of dynamics that usually accompany old or new relationships. Chris Argyris,[15] a management theorist, suggests that, over time, a group develops from an immature, passive state to a mature, self-directive state. Dependency of members on the group leader, passivity of individuals, a scarcity of overt verbal or nonverbal behaviors, inner-directed responses, short time perspective, and erratic, shallow interests characterize the behavior of the immature, passive group. The mature group, however, characteristically displays independence of the members from the leader, activity of group members, many overt verbal or nonverbal behaviors, outer-directed responses, long-range time perspective, and a deep, strong interest among members concerning the direction of the group.

Many problem-solving groups will exist for only short periods of time, and group maturity will most likely be minimal. In another setting, however, the group may be an ongoing problem-solving group that is very mature.

(F) Size of the Group The size of the group should be decided after considering organizational role, group functions, and group maturity. Although the size should reflect all of these factors, the optimum number of participants for problem-solving technique is between 6 and 10 persons. A group of this size allows for involvement and idea generation in a workable situation.

(G) Climate of the Group The climate of the group is also important for decision making. Certain behaviors are clues to the climate in the group. Members in a supportive group will offer positive reinforcement, stroking, smiling, head nodding, direct eye contact, forward body movement, and so on. Members in a hostile or nonsupportive environment will discount ideas and people, sigh deeply, frown, avoid eye contact, and behave passively. Passive behaviors in this situation are those that deny the problem.

(iii) Manager's Information Processing Styles

The quality of a decision is a direct reflection of how the decision maker processes information. Managers approach decision making and problem solving in very different ways, depending on their information processing styles. Their approaches, perceptions, and recommendations vary because their minds work differently. *Researchers have identified two general information-processing styles: (1) the thinking (analytic) style and (2) the intuitive style. One is not superior to the other.*

The **analytic style** managers tend to be logical, precise, and objective. They prefer routine assignments that require attention to detail and systematic implementation. The manager uses

[15] Chris Argyris, "Teaching Smart People How to Learn," *Harvard Business Review*, (May–June 1991).

deductive reasoning. The analytic style is good to use in model-building exercises and forecasting involving projections.

The **intuitive style** manager is creative, is comfortable in handling a dynamic and nonroutine environment, follows hunches, and is mostly subjective. This manager likes to address broad issues and use inductive reasoning. This manager sees things in complex patterns rather than as logically ordered bits and pieces. The intuitive style is good to use in brainstorming sessions and where traditional assumptions need to be challenged.

In practice, many managers process information through a combination of analytic and intuitive styles.

(iv) Stages of Group Development

Effectiveness and efficiency increase as the group matures. Similarly, immature groups are ineffective and inefficient. A significant benefit of group maturity is that a person's individuality strengthens. Also, members of mature groups tend to be emotionally mature.

Kreitner[16] suggests six stages of group development:

1. Orientation
2. Conflict and challenge
3. Cohesion
4. Delusion
5. Disillusion
6. Acceptance

During stages 1 through 3, group members attempt to overcome the obstacles of uncertainty over and authority, while during stages 4 through 6, they overcome the obstacles of uncertainty over interpersonal relations. An understanding of group development stages will improve time-management skills of an employee.

Stage 1: Orientation. Group members give the impression to managers and leaders that they want permanent control expressed through wants and needs.

Stage 2: Conflict and change. Group members struggle for control by suggesting alternative courses of action and strive to clarify and reconcile their roles. Many groups do not continue past this stage because they get bogged down due to emotionalism and political infighting. An "I" feeling is dominant at this stage for power and authority.

Stage 3: Cohesion. A "we" feeling becomes apparent at this stage as everyone becomes truly involved in the project and any differences over power and authority are resolved.

Stage 4: Delusion. Issues and problems are dismissed or treated lightly. Group members work in participation and promote harmony at all costs.

Stage 5: Disillusion. Disillusion sets in as unlimited goodwill wears off and disenchantment grows. Some members will prevail by showing their strengths while others hold

[16] Kreitner, *Management.*

back. Tardiness and absenteeism are the norm, which is symptomatic of diminishing cohesiveness and commitment.

Stage 6: Acceptance. Some group members move from conflict to cohesion and act as group catalysts as their expectations are more realistic. Power and authority structure is accepted. Consequently, the group members tend to be highly effective and efficient.

(v) Organizational Politics

Organizational politics (OP), impression management, focuses on self-interest in response to opposition at the workplace. Many employees feel that "freedom from office politics" is important to their job satisfaction. Positive aspects of OP include exchanging favors, forcing coalitions, and seeking sponsors at upper levels of the organization. Negative aspects of OP include whistle-blowing, revolutionary coalitions, threats, and sabotage.

Why do employees and employers promote OP? Employees resort to OP when they are unwilling to trust their career solely to competence, hard work, or luck. An organization's climate or culture placing unreasonable barriers to individual or group success promotes OP.

Research on OP has indicated that:

1. The larger the organization and the higher the levels of management, the greater the perceived amount of political activity.
2. People in staff positions were viewed as more political than those in line positions.
3. Marketing people were viewed as more political than those in production.
4. "Reorganization changes" prompted more political activity than any other types of change.

Examples of positive impact resulting from OP include gaining visibility for ideas, improving coordination and communication, developing teams and groups, advancing one's career, and increasing esprit de corps. Examples of negative impact resulting from OP include distraction from organizational goals, misuse of resources, and organizational conflict.

Tactics that are common expressions of OP in the workplace include posturing (one-upmanship), empire building, making the superior look good (apple polishing), political favors, creating power and loyalty cliques, reciprocating, engaging in destructive competition, and sabotaging (as a last resort).

Remedies to OP include creating openness and trust, measuring employee performance rather than personalities, integrating individual and organizational goals, implementing job rotation techniques, and practicing better work scheduling and timely career planning.

Rules for winning at OP include:

1. Finding out what the supervisor expects.
2. Finding out how the grapevine works.
3. Finding a mentor.
4. Fighting over major issues only.
5. Not hiring a family member or a close friend.

(vi) Criteria and Determinants of Group Effectiveness

A group is defined as two or more freely interacting individuals who share a common identity and purpose. Individuals join groups for various reasons to satisfy their personal and professional goals. Two kinds of groups exist: informal and formal groups. An informal group is a collection of individuals seeking friendship while a formal group is a collection of individuals doing productive work. Individuals can be subjected to ostracism, which is rejection from a group.

Two criteria for group effectiveness include attractiveness and cohesiveness. Attractiveness has the outside-looking-in view, while the cohesiveness has the inside-looking-out view. Cohesive group members tend to stick together as they focus on "we" instead of "I." An individual's perception and frames of reference have a lot to do with how groups can be attractive or cohesive.

Factors that can enhance a group's attractiveness and cohesiveness include cooperative relationships among members, a high degree of interaction among group members, a relatively small-size group, and similarities among group members.

Factors that can detract from a group's attractiveness and cohesiveness include unreasonable demands on the individual, disagreement over work rules and procedures, unpleasant experience with some group members, and destructive competition or conflict.

(vii) Management Structures and Organization Systems

In this section, we review two organization systems—closed system and open system—and two management structures—mechanistic and organic. A relationship between management structures and organization systems is established.

A closed system is independent of its external environment; it is autonomous, enclosed, and sealed off from the external environment. It focuses on internal systems only. Its external environment is simple, stable, and predictable. The major issue for management is to run the business efficiently with centralized decision making and authority. A closed system represents a bureaucratic organization.

An open system is dependent on its environment to survive; it both consumes resources and exports resources to the external environment. It transforms inputs into outputs. It must continuously change and adapt to the external environment. Open systems are complex, unstable, and unpredictable, and internal efficiency is a minor issue for management. Open systems represent modern organizations.

A mechanistic management structure is characterized by rules, procedures, and a clear hierarchy of authority. Organizations are formalized and centralized, and the external environment is stable.

An organic management structure is characterized by a fluid (looser) and free-flowing nature, which is adaptive to changes in the external environment with few or no written rules and regulations and operates without a clear hierarchy of authority. Organizations are informal and decentralized, and responsibility flows down to lower levels. An organic management structure encourages teamwork and problem solving by letting employees work directly with each other.

MANAGEMENT STRUCTURES AND ORGANIZATION SYSTEMS

- A mechanistic management structure resembles a closed system of an organization.
- An organic management structure resembles an open system of an organization.

(viii) Criteria and Determinants of Organizational Effectiveness

The next items are highlights of organizational effectiveness and organizational decline:

- Effectiveness is a measure of whether organizational objectives are accomplished or not.
- Efficiency is the relationship between outputs and inputs.
- The effectiveness criteria are prescribed by society in the form of explicit expectations, regulations, and laws and by stockholders in the form of profits, ROI, and growth.
- Organizational effectiveness has a time dimension to it (i.e., near, intermediate, and distant future).
- Organizational decline results from management complacency (usually the primary culprit), unsteady economic growth, resource shortages, competition, and weak demand for products and services. It typically involves a reduction in the size or scope of the organization.

Ways to prevent organizational decline are listed next.

- Organize the company into definable ventures that have explicit goals.
- Concentrate on the toughest competitors and the most difficult customers.
- Define each job so that it is closely tied to a venture.
- Promote individual diversity to take risks and experiment with new ideas.
- Strengthen the participative management process.
- Emphasize more effective information flow, both downward and upward.

(d) Human Resource Processes

A policy is a statement of how an organization intends to handle an issue or a situation.[17] A policy statement can be brief or expanded. A key element of a policy is that it is a predetermined guideline providing a specified course of action for dealing with prescribed circumstances. Some organizations operate without written policies because they want to handle issues on a case-by-case basis. Employees may see this as a way to show favoritism or discrimination. Unwritten practices tend to become informal policies causing confusion and chaos.

Two choices are available for companies who want to develop written policies: They can develop policies on a department level or on an organization level. Policies developed at the individual department level could create conflicting practices for common items such as attendance, promotions, vacations, sick leave, and employee discipline, leading to low productivity and high morale problems.

Policies developed on an organization level provide:

- Consistency in handling similar issues.
- Improved communication of policy issues.
- Control over personnel costs.
- Prevention or response to administrative claims and litigations.

[17] William S. Hubbartt, *Personnel Policy Handbook* (New York: McGraw-Hill, 1993).

- Compliance with government laws and regulations.
- Delegation of routine personnel decisions to supervisors and managers.

Exhibit 5.50 presents various types of organizational policies.

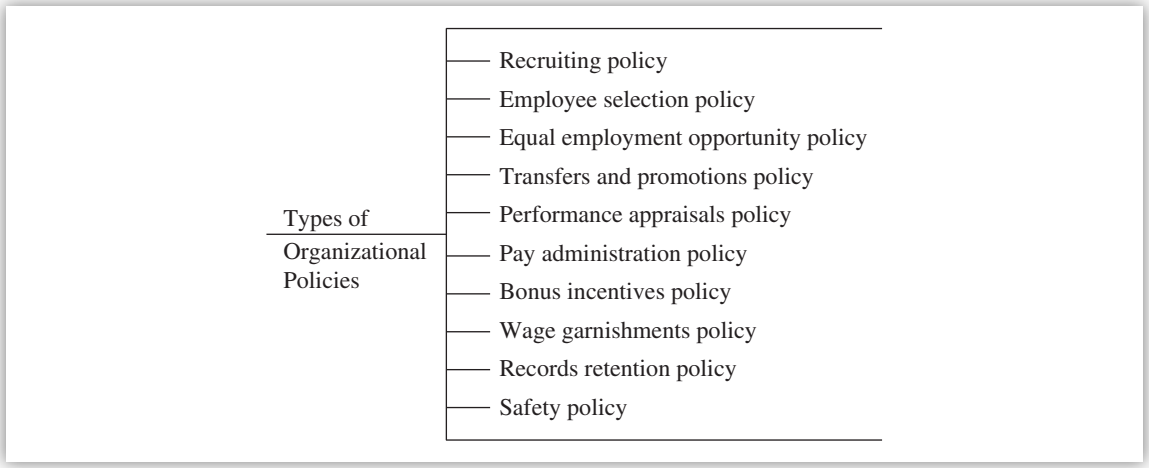


EXHIBIT 5.50 Types of Organizational Policies

(i) Recruiting Policy

(A) Policy Guidance An HR policy on recruiting will guide managers to hire the right person for the job. The primary purpose of the recruiting policy is to attract qualified candidates at a minimum cost and time. A recruiting policy also will enable the organization to contact a diverse variety of recruiting resources, which helps to avoid charges of bias in recruiting practices.

In the absence of a defined recruiting policy, hiring managers will do whatever method works best for attracting candidates. Some will ask employees for referrals, some will talk to employment agencies, while others will place an advertisement in the local paper. These efforts will produce varying results. Some recruiting methods will be more costly than others. A recruiting policy will help managers to achieve the best results.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Although hiring of applicants referred by current employees is a low-cost and effective means for recruiting employees, excessive reliance on this method can be counterproductive and even result in legal problems for the employer. Employee cliques would result in excessive turnover because newly hired workers would feel like outsiders.
- Failure to attract a diverse applicant pool could result in charges of employment discrimination by the Equal Employment Opportunity Commission (EEOC) as discriminating between minority and nonminority applicants. It is a good practice to communicate job opening information to all employees and to all outside communities through various media available.
- Conflict between the recruiting policy and the promotion-from-within policy could slow down and complicate the hiring process. For example, promotion policies complicate the

hiring process by delaying the filling of the job or requiring the promotion of a marginally qualified worker when a fully qualified applicant from outside the company is available.

(ii) Employee Selection Policy

(A) Policy Guidance Careful employee selection is an important activity because capable, hardworking employees affect the productivity and profitability of the organization. Careful selection involves employee screening, testing, physical exam, and orientation. Costs are incurred during selection, termination, and rehiring.

The objective of a policy on employee selection and testing is to provide guidelines on selection procedures that will help managers in selecting a qualified employee while avoiding legal liabilities. Policy guidance facilitates a uniform and thorough approach to employee selection. With selection guidelines, there is a great likelihood that supervisors will make better selection decisions.

In the absence of guidelines, managers will try different employee selection techniques. Some managers conduct detailed interviews. Others may ask only a few questions about job skills or personal interests and then make a hiring decision based on applicant personality. Some managers devise tests for applicants or ask applicants to demonstrate their skill at running a machine used on the job. At best, these techniques will have varying degrees of success; at worst, such practices have been shown to be improper and discriminatory selection devices. EEOC provides guidelines about employment tests, interviewer rating scales, and the regulation requirements that the test be a valid measure of required performance on the job.

JOB DESCRIPTIONS

A job description is useful in employee recruiting, screening, training, compensating, and evaluating performance. A written job description is needed to effectively analyze the job to determine its exempt or nonexempt status. Management is responsible for developing, using, and maintaining the job description. Job descriptions should not include gender-based terms (e.g., saleswoman) or arbitrary requirements (e.g., high school or college degree), which could be viewed as discriminatory and in violation of antibias laws. Job descriptions should include a disclaimer that asserts management's right to change job duties.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Polygraph testing for preemployment screening of applicants by nongovernmental employees is now a prohibited employment practice under the Polygraph Protection Act of 1990.
- The Americans with Disabilities Act (ADA) of 1990 states that in the event that an applicant with a disability is unable to complete a test due to the disability, the employer is responsible for making a reasonable accommodation by identifying an alternative means to permit the applicant to demonstrate the skill or knowledge that the test purports to measure.
- Avoid inquiries about physical or mental handicaps, age, sex, national origin, or other protected categories on the employment application.
- Avoid misunderstandings by confirming job offers in a letter that specifies job, start date, and pay rate.

- Use objective, job-related criteria throughout the selection process. Job descriptions are a useful tool in the selection process.
- Be consistent in the use of selection techniques. If a selection procedure, such as reference checks, physical exam, or drug screen, is used on one candidate, it should be used on all candidates for the same job or similar class of jobs. Sporadic use of a selection procedure could be viewed as a discriminatory hiring practice.
- Check employment classifications (e.g., exempt or nonexempt employee) to ensure that they do not create a category that groups employees by race, age, sex, or other protected class defined by antibias laws. Employment classifications help to sort out issues such as eligibility for benefits, payments of salaries, and entitlement to overtime pay.
- The preemployment physical exam is now prohibited by ADA. A postoffer physical exam is allowed as long as it is not used to screen out qualified disabled applicants. However, OSHA requires preemployment physical exams on certain jobs, such as employees working in a noisy environment. These applicants require a hearing test and periodic retesting.
- Avoid placing a new employee on a new job without complete orientation and training.
- Avoid telling a new employee that he or she will receive a salary adjustment after 30 or 60 days. Use the term "performance appraisal" instead of a "salary adjustment," where the latter term would imply an automatic increase in the salary.

KEY CONCEPTS TO REMEMBER: Job Analysis, Job Descriptions, and Job Specifications

- A **job analysis** is used to develop job descriptions and job specifications. The **development** function is the place where job analyses are done. The scope of a job analysis includes: (1) analyzing workflows and tasks, (2) observing employees work, (3) studying the methods used to attain work-unit objectives, and (4) interviewing employees about how they accomplish their tasks. The administration of a fair and equitable compensation program should be based on a current job analysis.

Job analysis → Job descriptions → Job specifications

- A **job/position description** is developed based on a job analysis. A job description includes a listing of job title, job duties, job requirements, and reporting relationships. It summarizes the duties that the employee will be held accountable for performing. Compensation rates are not included in job descriptions although they are developed simultaneously.
- A **job specification** document contains the job requirements in detail (which becomes a "core" of the job) and the minimum qualifications (e.g., education, experience, other skills) necessary to perform the job satisfactorily.

(iii) Equal Employment Opportunity Policy

(A) Policy Guidance A policy statement asserting equal employment opportunity, by itself, is not enough to prevent discriminatory practices. Since equal employment laws cover all employment decisions, specific guidelines are needed to guide managers in effectively implementing this policy.

A policy on equal employment opportunity must accomplish a variety of purposes. It must identify protected class employees, specify covered employment decisions, outline guidelines

for managers, provide a mechanism for individuals to present claims, and define procedures for resolution of those claims.

(B) Ways to Minimize Potential Risks and Exposures There are various ways to minimize potential risk and exposures. Some of them are listed next.

- Avoid using "boilerplate" equal employment policy and expect to be in full compliance with the law. For employees, management actions will speak much louder than words.
- Address nondiscrimination issues when writing personnel policies for recruiting, selection, training, promotions, pay administration, discipline, appraisals, discharges, and other policy areas.
- Implement all policies consistently for all employees. For example, excessive attention to or documentation of the discharge of a minority staffer when other cases are not similarly documented could be viewed as a discriminatory practice. Likewise, a company's failure to document the performance problems of a minority female staffer because of fear of a discrimination claim, and then subsequently terminating that individual, was judged to be a discriminatory employment practice.
- Issue separate policies on preventing sexual harassment or complying with disabilities act provisions in order to get special attention instead of combining with other policies of the organization.

Courts have held that a hostile or offensive working environment constitutes unlawful sexual harassment even if the employee bringing the suit suffers no economic or job benefit losses as a result of such harassment. The EEOC holds the employer accountable for controlling sexual harassment occurring between employees, supervisors, and subordinates, or customers if the employer knows or should have known of the conduct. The EEOC recommends that companies should take proactive measures to prevent sexual harassment by developing a policy and communicating information to employees.

AFFIRMATIVE ACTION VERSUS EQUAL EMPLOYMENT OPPORTUNITY

- Firms having a specified dollar volume of contracts with the federal government or some other government jurisdictions are subject to affirmative action requirements. These require a race–sex breakout of the workforce compared to a race–sex breakout of the area labor force.
- Equal employment opportunity policies specify nondiscriminatory and nonpreferential treatment for all candidates and employees.

(iv) Transfers and Promotions Policy

(A) Policy Guidance on Transfers Employee transfers can occur between jobs, work locations, operating shifts, or departments. Transfers may be initiated by the organization to move an employee to another assignment in response to staffing requirements. Employees may also request transfers. Transfers may be temporary or permanent.

A personnel policy on transfers helps to sort out these various issues and guide the reassignment of employees to other jobs. The process of transferring employees raises questions about pay

rates, shift differential pay, reporting relationships, and duration of assignments. Transfers can also result in relocation for employees and their families. If these issues are not resolved properly, the employee will not be fully effective and productive on the new job assignment, thus costing more than its benefits.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Do not give up the flexibility to make temporary transfers when needed to respond to unique business conditions. Protect the management prerogative to assign employees to special tasks.
- Make sure that employee availability for transfer is a condition of employment.
- Avoid hardships to employees by allowing employees to accept or reject the transfer.
- Customize the transfer policies to be responsive to employee needs as well as business requirements.

(C) Policy Guidance on Promotions For many employees, career advancements and the opportunity for greater earnings is a significant motivator, which can contribute to organizational loyalty. Promotion policies are generally seen as good for morale. Often employees seek employment at a particular firm because of career advancement potential. For these reasons, many organizations have a philosophy of trying to promote from within whenever possible (see Exhibit 5.51).

Advantages and disadvantages of promoting from within	Advantages and disadvantages of hiring an outsider
Advantages include increased motivation among employees, less expensive than hiring an outsider, and not difficult to identify proven performers	Advantages include bringing a new perspective to or fresh look at the problem and current experience, training, skill, and education
Disadvantages include possibility of social inbreeding	Disadvantages include more expensive than promoting from within and difficult to identify proven performers

EXHIBIT 5.51 Advantages and Disadvantages of Promoting from Within and Hiring an Outsider

While advantages of promoting from within are low cost and timeliness, some disadvantages include promotion dilemma (i.e., when two equally qualified subordinates were under consideration for the job), low employee morale, and low productivity if the company disregards qualified employees to hire an outsider.

(D) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Use job-bidding promotion procedures so that only interested employees will come forward to apply.
- Post all jobs covered by the policy on the bulletin board. Failure to post jobs would lead to charges of favoritism. Posting the job and interviewing all candidates allows management to evaluate candidates and counsel those who are not selected.

(v) Performance Appraisals Policy

(A) Policy Guidance A performance appraisal is a structured discussion between employee and supervisor. It provides an opportunity for the supervisor to recognize an employee's achievements, offer suggestions for improvement when needed, discuss job responsibilities, define job objectives, counsel on career advancements, and justify a pay adjustment.

A policy on performance appraisals provides guidelines for managers to conduct effective performance appraisal. The policy can identify when performance appraisals should be scheduled, who is responsible for preparation of the appraisal, how the appraisal influences pay adjustments, and how to prepare for and conduct performance appraisals.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Use the objective data of performance results rather than subjective opinions. Recognition of good performance can be a motivation for employees. Likewise, when the employee performs poorly, the manager should rate the employee accordingly. If the manager fails to identify poor performance, the employee is likely to assume that performance is satisfactory, unless told otherwise.
- Consider separating performance appraisals and pay discussions. Otherwise, there is a great likelihood that the employee may think that both of them are the same.
- Avoid low rating from "hard" managers compared to high ratings from "easy" managers. One way to reduce this kind of inconsistency is to include performance-level definitions in the performance appraisal policy guidelines. Another approach is to have the appraisal form reviewed by the HR specialist.
- Conduct the performance appraisals on time to reduce employee anxiety and tension. This can be achieved by having the HR specialist remind the functional manager about due dates and monitor appraisal for on-time completion.

(vi) Pay Administration Policy

(A) Policy Guidance A pay administration policy provides instructions to aid supervisors in understanding the organization's compensation philosophy, formulating pay offers, and having salary adjustments. Further, it can define guidelines that allow supervisors to make pay decisions within prescribed limits. Exceptions to pay policy can be referred to HR management for approval.

SEQUENCE OF ACTIVITIES IN PAY ADMINISTRATION

- Perform job analysis.
- Develop job description.
- Conduct job evaluation.
- Determine salary ranges or pay levels.
- Conduct performance appraisal.

An organization's compensation philosophy sets the direction for its pay policy. The pay philosophy determines whether the firm is going to be a pay leader or follower, or match competitive norms. Many large firms tend to have defined compensation programs with formalized job evaluation systems and salary ranges. A plan of job classification is the basic element of compensation analysis and job evaluation.

A carefully defined pay administration policy also helps an organization comply with the Equal Pay Act of 1963. This act prohibits unequal wages for women and men who work in the same company performing substantially equal work with respect to skill, effort, and responsibility under similar working conditions.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Minimize the likelihood of inequity in pay rates by having an HR or compensation specialist review all pay offers and pay adjustments. The specialist should advise the supervisor if pay rates or pay ranges are unusually high or low.
- Improve control and consistency by defining a pay structure. The process for preparing a pay structure includes job evaluation, comparison of pay to an area salary survey, and creation of pay ranges. This process provides an objective basis to define job levels.

KEY CONCEPTS TO REMEMBER: Pay Plans

Four different pay plans exist: all-salary, skill-based evaluation, lump-sum salary increases, and cafeteria benefits. Advantages, disadvantages, and possible outcomes for each pay plan are presented next.

1. **All-salary.** Advantages include: promotes a climate of trust and produces increased satisfaction and job attraction. Disadvantages include: possible higher costs of administration and possible greater absenteeism. Possible favorable outcomes include: supervisors will deal with absenteeism, will produce participative climate, will create a responsible workforce, and jobs will be well designed.
2. **Skill-based evaluation.** Advantages include: promotes a more flexible and skilled workforce, promotes increased satisfaction, and promotes a climate of growth. Disadvantages include: higher costs of training and higher salaries. Possible favorable outcomes include: employees will want to develop themselves, and pay would be related to performance.
3. **Lump-sum salary increases.** Advantages include: provides increased pay satisfaction and provides greater visibility of pay increases. Disadvantages include: higher cost of administration and short-term salary inequities. Possible favorable outcomes include: provides fair pay rates and pay would be related to performance.
4. **Cafeteria benefits.** Advantages include: provides increased pay satisfaction and provides greater job attraction. Disadvantages include: higher cost of administration and possible lack of employee knowledge on various options. Possible favorable outcomes include: will provide a well-educated, heterogeneous workforce and provides good processing of data.

Source: Institute of Internal Auditors, *CIA Exam, Questions and Suggested Solutions*, Part III, Question 51 (Altamonte Springs, FL: IIA, May 1989).

(vii) Bonus Incentives Policy

(A) Policy Guidance Many organizations have considered bonus or incentive pay plans as a way to stimulate desired improvements in productivity and quality levels. The goal of a bonus incentive plan is to reward employees for achievement of specified performance results. It is a win-win situation—the employees benefit from higher compensation based on their attainment of plan objectives. The employer benefits because increased productivity (or lower costs) promotes higher profits. A good bonus plan should pay for itself.

Varieties of incentive pay plans follow. Premium pay is used by some firms to provide an incentive for certain kinds of work. Premium pay is added to the employee's base pay when certain specified conditions are met. Piece rate is often used in manufacturing firms where employee productivity is measured by the number of pieces produced. Many salespeople are compensated on a commission basis. The commission is a designated percentage of the selling price or profits on the items sold. Bonus incentives can be an informal payout to employees after a profitable year based on management discretion.

(B) Ways to Minimize Potential Rrisks and Exposures Various ways to minimize potential risks and exposures are listed next.

- A poorly designed bonus plan or unattainable incentive goals will be demotivating.
- Recognize that a bonus incentive plan can cause employees to focus activities solely toward the specified bonus incentive factor, at the expense of other job activities. To balance this conflict situation, both quality and quantity goals should be emphasized.
- Consider implementing two types of bonus incentive plans: one on an individual basis and the other based on group. An individual incentive coupled with a group incentive plan helps promote teamwork throughout the organization and achieve a balance between individual and group goals.

(viii) Wage Garnishments Policy

(A) Policy Guidance Wage garnishments are a court-ordered process for an employer to withhold a portion of an employee's earnings for payment of a debt. Therefore, the garnishments impose a legal obligation upon the employer. An employer's failure to withhold monies as directed could create financial obligations on the company. Further, failure to properly handle deductions can create legal liabilities for the firm. For these reasons, it is important to define a policy to guide the handling of wage deduction orders.

There are a variety of wage deduction orders: tax liabilities (back taxes) to tax authorities, spouse or dependent (child) support payments, and creditors based on wage assignment agreement when granting credit.

The Consumer Credit Protection Act is one law that defines employer obligations relating to wage garnishments. The act prohibits employers from discharging an employee whose earnings have been subjected to any one indebtedness. Further, the law limits the amount of an employee's wages that can be subject to garnishments.

Until the Hatch Act was amended in February 1994, the federal government agencies were exempted to collect wages from federal government employees for debts incurred outside their

employment. The amended act requires federal agencies to honor court orders for withholding amounts of money from an employee's wages and to make payment of that withholding to another person or organization for the specific purpose of satisfying a legal debt of the employee. The total debt can include recovery of attorney's fees, interest, or court costs.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- The employer will incur extra costs for handling the wage garnishment orders. As a result, employers may be upset with the employee or with the system and take inappropriate action, creating legal liabilities.
- Do not be tempted to fire the employee when a wage garnishment order is received.
- Be alert for official-looking letters from collections agencies demanding wage deductions to pay off indebtedness.
- Specify a priority sequence for handling multiple garnishments received on the same employee. For example, an IRS tax garnishment takes priority over all others, then support garnishment, and then garnishment for other debts. Garnishment orders should be processed one at a time in the order received. When two or more garnishments are received, notify the later creditors that their demand notices will be satisfied upon completion of prior notices.

(ix) Records Retention Policy

(A) Policy Guidance Federal government labor laws, wage hour laws, and many similar state laws specify certain minimum records that must be maintained by employers. These laws define minimum records retention requirements. Some states have laws that deal with the issues of personnel records privacy and employee access to personnel files.

A policy on HR records is important for these reasons: to maintain accurate records, to retain records required by law, and to protect records' confidentiality. For example, with accurate personnel records that reflect the individual's education, experience, job history, and performance levels, management can make more informed personnel decisions. Other advantages of accurate personnel records include helping a company to prevail in unemployment compensation hearings and providing a basis for defending against discrimination charges or wrongful discharge lawsuits.

(B) Ways to Minimize Potential Risks and Exposures Various ways to minimize potential risks and exposures are listed next.

- Protect the confidentiality of personnel records by keeping files in locked drawers or file cabinets and requiring access codes to access computer-based records and by changing these access codes periodically.
- Avoid the tendency to allow supervisors unrestricted latitude in responding to reference check inquiries by other area employers. A former employee can file a lawsuit because of poor handling of employment references. An untrained supervisor carelessly giving a bad reference about a former employee could create a liability for a libel or defamation lawsuit. The best preventive action is to send reference inquiries to the personnel records specialist. Release references only in response to written inquiries. Limit the reference check to verifying dates of employment and job title(s) and confirming salary if the other employer

provided data given by the employee. Avoid detailed subjective evaluation of unverifiable performance information.

- Avoid unnecessary restrictions on employees viewing their own files. When permitting an employee to view his or her file, the viewing should take place in the presence of a supervisor, manager, or HR specialist. This prevents unauthorized removal of documents from or insertion of documents into the employee file.

(x) Safety Policy

Firms that have successful safety programs typically share three common characteristics: a management commitment to safety, active employee participation in safety activities, and thorough investigation of accidents. Successful safety programs reduce accidents. Fewer accidents mean less work interruptions, fewer worker's compensation claims, and lower insurance costs.

OSHA is the federal government agency responsible for defining and enforcing job standards. The OSHA law covers all employers engaged in a business affecting commerce but excludes self-employed individuals, family firms, and workplaces covered by other federal safety laws. Employers covered by OSHA have a general duty to maintain a safe and healthful workplace. The general duty requirements mean that the employer must become familiar with safety standards that affect the workplace, educate employees on safety, and promote safe practices in the daily operation of the business.

MANUFACTURING OPERATIONS AUDIT

In a manufacturing operations audit, the audit objective was to determine whether all legal and regulatory requirements concerning employee safety are being properly implemented. The audit procedure would be to examine documentation concerning the design and operation of the relevant systems and to observe operations for compliance.

(A) Safety Responsibility A safety responsibility policy serves as the framework for additional policy guidelines that direct safety activities. Typical safety activities include safety orientation, safety training, safety committee, workplace inspections, and accident investigations. Also effective in promoting safe work practices are safe operating procedures, job safety analysis, and publishing of safety rules. In order to implement this policy, a safety manager should be designated to coordinate day-to-day safety activities and should be supported by higher-level management for having ultimate responsibility for directing workplace safety.

Safety policy guidelines provide a basis for promoting employee participation in safety activities. Active participation in safety is one important way to keep safety in everyone's mind. A safety mind-set helps to prevent accidents.

Some risks that could result from noncompliance, or pitfalls to avoid, include not holding supervisors and managers accountable for safety in their respective work areas, not including safety results on a supervisor's performance evaluation, and a tendency to publish a few safety rules and then let things slide. Under the law, an employer will be held liable for failing to enforce safety rules. If a company publishes a safety rule but neglects to require employees to comply with the rule, the firm may be subject to a citation.

(B) Accident Investigation The purpose of accident investigation is to identify the accident's cause so that future accidents can be avoided. In addition to prevention of accidents, accident investigations serve several other important functions, such as:

- Eliminating unsafe conditions.
- Identifying training needs.
- Redesigning jobs.
- Preventing or combating fraud related to unethical worker's compensation claims.
- Analyzing accident data.
- Reporting to government.

(e) Risk/Control Implications of Different Leadership Skills

(i) Overview

The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed.[18] It also influences control activities, information and communication systems, and monitoring activities. This is true not only of their design but also the way they work day to day. The entity's history and culture influence the control environment. It influences the control consciousness of its people. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive tone at the top of management hierarchy (i.e., tone at the top). They establish appropriate policies and procedures, often including a written code of conduct, which foster shared values and teamwork in pursuit of the entity's objectives.

If management style is autocratic and the level of formality is highly structured, one can expect a strong control consciousness. Similarly, if management style is empowered and the level of formality is loose or informal, one can expect a weak control consciousness.

(ii) Control Environment Factors

The control environment encompasses seven factors (see Exhibit 5.52). Although all are important, the extent to which each is addressed will vary with the entity. For example, the chief executive of an entity with a small workforce and centralized operations may not establish formal lines of responsibility and detailed operating policies but could nevertheless have an appropriate control environment.

(A) Integrity and Ethical Values An entity's objectives and the way they are achieved are based on preferences, value judgments, and management styles. Those preferences and value judgments, which are translated into standards of behavior, reflect management's integrity and its commitment to ethical values.

The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other internal control components. *Integrity is a prerequisite for ethical behavior in all aspects of an*

[18] COSO, "Internal Control—Integrated Framework."

enterprise's activities. The CEO usually is the dominant personality in an organization and often individually sets its ethical tone.

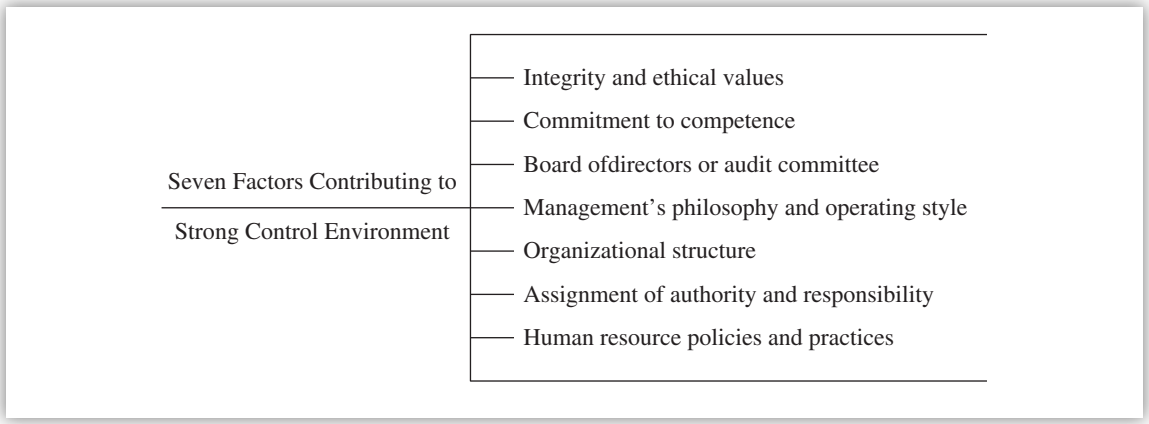


EXHIBIT 5.52 Seven Factors Contributing to Strong Control Environment

INCENTIVES AND TEMPTATIONS

Incentives cited for engaging in fraudulent or questionable financial reporting practices and, by extension, other forms of unethical behavior are:

- Pressure to meet unrealistic performance targets, particularly for short-term results.
- High performance-dependent rewards.
- Upper and lower cutoffs on bonus plans.

Temptations for employees to engage in improper acts include:

- Nonexistent or ineffective controls, such as poor segregation of duties in sensitive areas, that offer temptations to steal or to conceal poor performance.
- High decentralization that leaves top management unaware of actions taken at lower organizational levels and thereby reduces the chances of getting caught.
- A weak internal audit function that does not have the ability to detect and report improper behavior.
- An ineffective board of directors that does not provide objective oversight of top management.
- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents.

Source: Kenneth A. Merchant, *Fraudulent and Questionable Financial Reporting: A Corporate Perspective* (Morristown, NJ: Financial Executives Research Foundation, 1987).

An auditor should consider the control environment factor "integrity and ethical values" in determining whether a positive and effective control environment exists. Some issues that an auditor might focus on during a control evaluation are listed next.

- Existence and implementation of codes of conduct and other policies regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behavior

- Dealings with employees, suppliers, customers, investors, creditors, insurers, competitors, and auditors (e.g., whether management conducts business on a high ethical plane, and insists that others do so, or pays little attention to ethical values)
- Pressure to meet unrealistic performance targets—particularly for short-term results—and extent to which compensation is based on achieving those performance targets

(B) Commitment to Competence Competence should reflect the knowledge and skills needed to accomplish tasks that define the individual's job. There often is a trade-off between competence and cost. Management needs to specify the competence levels for particular jobs and to translate those levels into requisite knowledge and skills. The necessary knowledge and skills may in turn depend on the individuals' intelligence, training, and experience. There often can be a trade-off between the extent of supervision and the requisite competence level of the individual.

An auditor should consider the control environment factor "commitment to competence" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus during control evaluation are listed next.

- Formal or informal job descriptions or other means of defining task that comprise particular jobs
- Analyses of the knowledge and skills needed to perform jobs adequately

(C) Board of Directors or Audit Committee The entity's board of directors and audit committee influences the control environment and tone at the top significantly. Factors include the board or audit committee's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and the appropriateness of its actions. Another factor is the degree to which difficult questions are raised and pursued with management regarding plans or performance. Interaction of the board or audit committee with internal and external auditors is another factor affecting the control environment.

An auditor should consider the control environment factor "board of directors or audit committee" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus during control evaluation include:

- Independence from management, such that necessary, even if difficult and probing, questions are raised.
- Frequency and timeliness with which meetings are held with chief financial and/or accounting officers, internal auditors, and external auditors.
- Sufficiency and timeliness with which information is provided to board or committee members, to allow monitoring of management's objectives and strategies, the entity's financial position and operating results, and terms of significant agreements.
- Sufficiency and timeliness with which the board or audit committee is apprised of sensitive information, investigations, and improper acts (e.g., travel expenses of senior officers, significant litigation, investigation of regulatory agencies, defalcations, embezzlement or misuse of corporate assets, violations of insider trading rules, political payments, illegal payments).

KEY CONCEPTS TO REMEMBER: Control Environment

- The primary purpose of an internal auditor's evaluation of internal controls is to determine if management has planned and implemented activities needed to attain goals and objectives.
- Control by management is the result of proper and effective planning, organizing, and directing of organizational activities.
- Adequate control is defined as a state that exists if management has planned and organized in a manner that provides reasonable assurance that the organization's objectives and goals will be achieved efficiently and economically.
- Controls provide assurance to management that desired actions will be accomplished when objectives are established in writing, standards are adopted, results are compared with the standards, and corrective actions are undertaken.
- Corporate directors, management, external auditors, and internal auditors all play important roles in creating a proper control environment. Senior management is primarily responsible for establishing a proper environment and specifying an overall internal control structure.
- Corporate management has a role in the maintenance of internal control. In fact, management sometimes is a control. For example, supervision of employees is a control device.
- An adequate system of internal controls is most likely to detect an irregularity perpetrated by a single employee, not a group of employees in collusion.
- It is control weakness when the audit committee of the board consists of the chief executive officer, the chief financial officer, and a major stockholder.
- Accounting and auditing are control-oriented functions in an organization. While management accountants prepare reports to senior management detailing the funds expended and the expenses incurred by each department in the company, internal auditors would identify inadequate controls that increase the likelihood of unauthorized expenditures.
- A control strength environment is where the treasurer's office prepares checks for suppliers based on vouchers prepared by the accounts payable department.
- The internal audit's overall responsibility is to act as an independent appraisal function to review operations as a service to management by measuring and evaluating the effectiveness of controls.

(D) Management's Philosophy and Operating Style Management's philosophy and operating style affect the way the enterprise is managed, including the kinds of business risks accepted. An entity that has been successful taking significant risks may have a different outlook on internal control than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory. An informally managed company may control operations largely by face-to-face contact with key managers. A more formally managed one may rely more on written policies, performance indicators, and exception reports.

Other elements of management's philosophy and operating style include attitudes toward financial reporting, conservative or aggressive selection from available alternative accounting principles, conscientiousness and conservatism with which accounting estimates are developed, and attitudes toward data processing and accounting functions and personnel.

An auditor should consider the control environment factor "management's philosophy and operating style" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus on during control evaluation include:

- Nature of business risks accepted (e.g., whether management often enters into particularly high-risk ventures or is extremely conservative in accepting risks).
- Frequency of interaction between senior management and operating management, particularly when operating from geographically removed locations.
- Attitudes and actions toward financial reporting, including disputes over application of accounting treatments (e.g., selection of conservative versus liberal accounting policies; whether accounting principles have been misapplied, important financial information has not been disclosed, or records have been manipulated or falsified).

(E) Organizational Structure An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Activities may relate to what is sometimes referred to as the value chain: inbound (receiving) activities, operations, or production, outbound (shipping), marketing, sales and service.

Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. An entity develops an organizational structure suited to its needs. Some are centralized; others are decentralized. Some have direct reporting relationships; others are more of a matrix organization. Some entities are organized by industry or product line, by geographical location, or by a particular distribution or marketing network. Other entities, including many state and local governmental units and not-for-profit institutions, are organized on a functional basis.

An auditor should consider the control environment factor "organizational structure" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus during control evaluation include:

- Appropriateness of the entity's organizational structure and its ability to provide the necessary information flow to manage its activities.
- Adequacy of definition of key managers' responsibilities and their understanding of these responsibilities.
- Adequacy of knowledge and experience of key managers in light of responsibilities.

(F) Assignment of Authority and Responsibility An entity can assign authority and responsibility for operating activities and establishing reporting relationships and authorization protocols. It involves the degree to which individuals and teams are encouraged to use initiative in addressing issues and solving problems as well as limits of their authority. It also deals with policies describing appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

EMPLOYEE EMPOWERMENT

There is a tendency to push authority downward to bring decision making closer to front-line personnel. An entity may take this tack to become more market driven or quality focused—perhaps to eliminate defects, reduce cycle time, or increase customer satisfaction.

Alignment of authority and accountability often is designed to encourage individual initiative, within limits. Delegation of authority, or "empowerment," means surrendering central control of certain business decisions to lower echelons—to the individuals who are closest to everyday business transactions. This may involve empowerment to sell products at discount prices; negotiate long-term supply contracts, licenses, or patents; or enter alliances or joint ventures.

A critical challenge is to delegate only to the extent required to achieve objectives. Doing this requires ensuring that risk acceptance is based on sound practices for identification and minimization of risk, including sizing risks and weighing potential losses against gains in arriving at good business decisions.

Another challenge is ensuring that all personnel understand the entity's objectives. It is essential that each individual know how his or her actions interrelate and contribute to achievement of the objectives.

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true all the way to the chief executive, who has ultimate responsibility for all activities within an entity, including the internal control system.

An auditor should consider the control environment factor "assignment of authority and responsibility" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus on during control evaluation include:

- Assignment of responsibility and delegation of authority to deal with organizational goals and objectives, operating functions, and regulatory requirements, including responsibility for information systems and authorizations for changes.
- Appropriateness of control-related standards and procedures, including employee job descriptions.
- Appropriate numbers of people, particularly with respect to data processing and accounting functions, with the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems.

(G) Human Resource Policies and Practices HR practices send messages to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example:

- Standards for hiring the most qualified individuals, with an emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people.
- Recruiting practices that include formal, in-depth employment interviews and informative and insightful presentations on the entity's history, culture, and operating style send a message that the entity is committed to its people.
- Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars, simulated case studies, and role-play exercises illustrate expected levels of performance and behavior.
- Rotation of personnel and promotions driven by periodic performance appraisals demonstrate the entity's commitment to the achievement of qualified personnel to higher levels of responsibility.

- Competitive compensation programs that include bonus incentives serve to motivate and reinforce outstanding performance.
- Disciplinary actions send a message that violations of expected behavior will not be tolerated.

It is essential that personnel be equipped for new challenges as issues that enterprises face change and become more complex, driven in part by rapidly changing technologies and increasing competition. Education and training, whether classroom instructions, self-study, or on-the-job training, must prepare an entity's people to keep pace and deal effectively with the evolving environment. They will also strengthen the entity's ability to effect quality initiatives. Hiring of competent people and one-time training are not enough. The education process must be ongoing.

An auditor should consider the control environment factor "human resource policies and practices" in determining whether a positive and effective control environment exists. Some issues on which an auditor might focus during control evaluation include:

- Extent to which policies and procedures for hiring, training, promoting, and compensating employees are in place.
- Appropriateness of remedial action taken in response to departures from approved policies and procedures.
- Adequacy of employee candidate background checks, particularly with regard to prior actions or activities considered being unacceptable by the entity.
- Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g., performance evaluations) and relation to the code of conduct or other behavioral guidelines.

5.3 Management Skills

In this section, topics such as leadership skills and group synergy through team building are presented.

(a) Leadership Skills

(i) Management Skills Defined

Management skills can be broadly classified as conceptual, human, and technical. These skills are not exhibited equally across management levels. They vary with the nature of the job, the level of decision making, and the type of interaction with people.

Conceptual skill is the cognitive ability to see the organization as a whole and the relationship among its parts. It involves the manager's thinking, information processing, and planning. It requires the ability to think strategically—to take the broad, long-term view. Conceptual skills are needed by all managers but are especially important for managers at the top. Many of the responsibilities of top managers, such as decision making, resource allocation, and innovation, require a broad view.

Human skill is the manager's ability to work with and through other people and to work effectively as a group member. It includes the ability to motivate, facilitate, coordinate, lead, communicate,

and resolve conflicts. As globalization, workforce diversity, uncertainty, and competition for highly skilled knowledge workers increase, human skills become even more crucial. Here, focus is on emotional needs of employees instead of the physical needs related to the job.

Technical skill is the understanding of and proficiency in the performance of specific tasks. It includes mastery of the methods, techniques, and equipment involved in specific functions such as engineering, manufacturing, or finance. These skills are particularly important at lower organizational levels. Many managers get promoted to their first management job by having excellent technical skills. However, technical skills become less important than human and conceptual skills as managers move up the hierarchy.

The next list presents a highest-to-lowest order of importance of these skills for three types of management levels.

1. First-line supervisor: Technical, human, conceptual
2. Middle-level manager: Human, technical, conceptual
3. Senior-level manager: Human, conceptual, technical

(ii) Management Functions and Types

(A) Management Functions Management is the attainment of organizational goals in an effective and efficient manner through planning, organizing, leading, and controlling organizational resources. There are two important ideas in this definition: (1) the four functions of planning, organizing, leading (directing), and controlling; and (2) the attainment of organizational goals in an effective and efficient manner. Managers use a multitude of skills to perform these functions.

- **Planning.** Planning defines where the organization wants to be in the future and how to get there. Planning means defining goals for future organizational performance and deciding on the tasks and use of resources needed to attain them. A lack of planning—or poor planning—can hurt an organization's performance.
- **Organizing.** Organizing typically follows planning and reflects how the organization tries to accomplish the plan. Organizing involves the assignment of tasks, the grouping of tasks into departments, and the assignment of authority and allocation of resources across the organization.
- **Leading.** Providing leadership is becoming an increasingly important management function. Leading is the use of influence to motivate employees to achieve organizational goals. Leading means creating a shared culture and values, communicating goals to employees throughout the organization, and infusing employees with the desire to perform at a high level. Leading involves motivating entire departments and divisions as well as those individuals working immediately with the manager. In an era of uncertainty, international competition, and a growing diversity of the workforce, the ability to shape culture, communicate goals, and motivate employees is critical to business success.

  One doesn't have to be a well-known top manager to be an exceptional leader. Many managers working quietly also provide strong leadership within departments, teams, not-for-profit organizations, and small businesses.
- **Controlling.** Controlling is the fourth function in the management process. Controlling means monitoring employees' activities, determining whether the organization is on

target toward its goals, and making corrections as necessary. Managers must ensure that the organization is moving toward its goals. New trends toward empowerment and trust of employees have led many companies to place less emphasis on top-down control and more emphasis on training employees to monitor and correct themselves.

New information technology is also helping managers provide needed organizational control without strict top-down constraints. Companies may also use information technology to put *more* constraints on employees if managers believe the situation demands it. Organization failure can result when managers are not serious about control or lack control information.

(B) Management Types Managers use conceptual, human, and technical skills to perform the four management functions of planning, organizing, leading, and controlling in all organizations. But not all managers' jobs are the same. Managers are responsible for different departments, work at different levels in the hierarchy, and meet different requirements for achieving high performance. Two management types include vertical differences and horizontal differences.

Vertical Differences An important determinant of the manager's job is hierarchical level. Three levels in the hierarchy include top managers, middle managers, and front-line (first-line) managers. Top managers are responsible for setting organizational goals, defining strategies for achieving them, monitoring and interpreting the external environment, and making decisions that affect the entire organization. They share a long-term vision for the organization, shape corporate culture, and nurture an entrepreneurial spirit that can help the company keep pace with rapid change. Middle managers are responsible for implementing the overall strategies and policies defined by top managers. They are concerned with the near future and are expected to establish good relationship with peers around the organization, encourage teamwork, and resolve conflicts. First-line managers are directly responsible for the production of goods and services. They include titles such as supervisor, line manager, section chief, and office managers. Their primary concern is the application of rules and procedures to achieve efficient production, provide technical assistance, and motivate subordinates. The time horizon in which they work is short, with the emphasis on accomplishing day-to-day goals.

Horizontal Differences The other major difference in management jobs occurs horizontally across the organization. These jobs include functional managers and general managers. Functional mangers are responsible for departments that perform a single functional task and have employees with similar training and skills. Line managers are responsible for the manufacturing (operations) and marketing departments that make or sell the product or service. Staff managers are in charge of departments such as finance and HR that support the line managers. General managers are responsible for several departments that perform different functions. Project managers also have general management responsibility, because they coordinate people across several departments to accomplish a specific project.

(iii) Managerial Roles

Henry Mintzberg[19] studied what managers do by focusing on the key roles they play. He criticized the traditional, functional approach as unrealistic and because it does not tell what managers actually do. Mintzberg believed that the functional approach portrays the management process as far more systematic and rational and less complex than it really is.

[19] Henry Mintzberg, "Managerial Work: Analysis from Observation," *Management Science* (October 1971).

In his view, the average manager is not the reflective planner and precise "orchestra leader" that the functional approach suggests. Mintzberg used a method called "structured observation," which included recording the activities and correspondence of few selected top-level executives. He then isolated 10 roles he believed are common to all managers. These 10 roles have been grouped into three major categories: (1) interpersonal, (2) informational, and (3) decisional roles (see Exhibit 5.53).

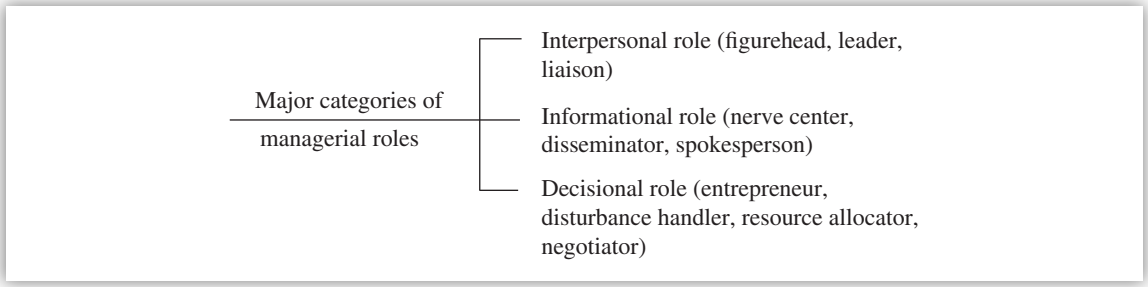


EXHIBIT 5.53 Major Categories of Managerial Roles

(A) Interpersonal Roles Because of their formal authority and superior status, managers engage in a good deal of interpersonal contact, especially with subordinates and peers. The three interpersonal roles that managers play are described next.

- **Figurehead.** As a symbol of legal authority, performing certain ceremonial duties (e.g., signing documents and receiving visitors)
- **Leader.** Motivating subordinates to get the job done properly
- **Liaison.** Serving as a link in a horizontal and vertical chain of communication

(B) Informational Roles Every manager is a clearinghouse for information relating to the task at hand. Informational roles are important because information is the heart of organizational decision making. Typical roles are described next.

- **Nerve center.** Serving as a focal point for nonroutine information; receiving all types of information
- **Disseminator.** Transmitting selected information to subordinates
- **Spokesperson.** Transmitting selected information to outsiders

(C) Decisional Roles In their decisional roles, managers balance conflicting interests and make choices. Through decisional roles, strategies are formulated and put into action. Four decisional roles are described next.

1. **Entrepreneur.** Designing and initiating changes within the organization
2. **Disturbance handler.** Taking corrective action in nonroutine situations
3. **Resource allocator.** Deciding exactly who should get what resources
4. **Negotiator.** Participating in negotiating sessions with other parties (e.g., vendors and unions) to make sure the organization's interests are adequately represented

(iv) Leadership Theories

The evolution of leadership theory can be presented in four ways: (1) trait theory, (2) behavioral style theory, (3) situational theory, and (4) transformational theory (see Exhibit 5.54).

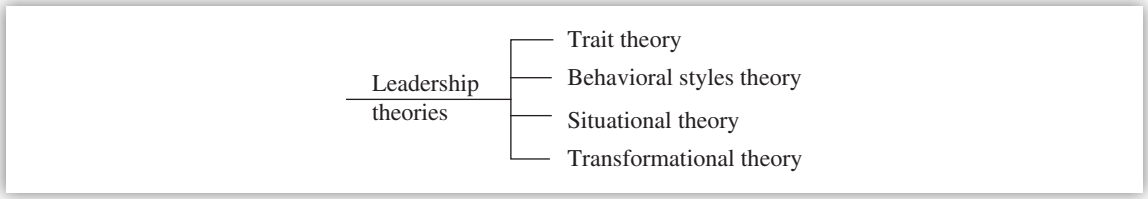


EXHIBIT 5.54 Leadership Theories

(A) Trait Leadership Theory It was assumed that leaders are born, not made. Later, this assumption was changed to accept that leadership traits are not completely inborn but can also be acquired through learning and experience.

Although hundreds of physical, mental, and personality traits were said to be the key determinants of successful leadership, researchers reached agreement on only five traits:

1. Intelligence
2. Scholarship
3. Dependability in exercising responsibilities
4. Activity and social participation
5. Socioeconomic status

Trait profiles do provide a useful framework for examining what it takes to be a good leader.

SURVEY OF MANAGERIAL TRAITS

Managers from across the United States were surveyed to determine the traits they admired in superior leaders. Results indicate:

- 87% selected honesty.
- 74% selected competent.
- 67% selected forward looking.
- 61% selected inspiring.
- 46% selected intelligent.

(B) Behavioral Styles Leadership Theory Researchers began turning their attention to patterns of leader behavior instead of concentrating on the personal traits of successful leaders. In other words, attention turned from who the leader was to how the leader actually behaved. Subordinates preferred managers who had a democratic style to those with an authoritarian style or a laissez-faire (hands-off) style. Exhibit 5.55 presents strengths and weaknesses of behavioral styles leadership theory.

Strengths of behavioral styles theory	Weaknesses of behavioral styles theory
Authoritarian style stresses prompt, orderly, and predictable performance.	Authoritarian approach tends to stifle individual initiative.
Democratic style enhances personal commitment through participation.	Democratic process is time consuming. This style does not always stimulate better performance. Some employees prefer to be told what to do rather than to participate in decision making.
Laissez-faire permits self-starters to do things as they see fit without leader interference.	Laissez-faire group may drift aimlessly in the absence of direction from leader.

EXHIBIT 5.55 Strengths and Weaknesses of Behavioral Styles Leadership Theory

Two popular models that have received a great deal of attention are the Ohio State Model and the Leadership Grid by Robert R. Blake and Jane Srygley Mouton.[20]

Ohio State Model A team of Ohio State University researchers defined two independent dimensions of leader behavior.

Dimension 1: Initiating structure (x-axis from low to high). This dimension represents the leader's efforts to get things organized and get the job done.

Dimension 2: Consideration (y-axis from low to high). This dimension is the degree of trust, friendship, respect, and warmth that the leader extends to subordinates.

A matrix was drawn from these two dimensions. High-structure, high-consideration was generally hailed as the best all-around style.

Leadership Grid Blake and Mouton[21] remain convinced that there is one best style of leadership. They described this in a grid with two axes.

1. **Horizontal (x) axis.** Concern for production involving a desire to achieve greater output, cost effectiveness, and profits
2. **Vertical (y) axis.** Concern for people involving promoting friendship, helping coworkers get the job done, and attending to things that matter to people, such as pay and working conditions

By scaling each axis from 1 to 9, the grid consists of these five leadership styles:

1. **9, 1 style.** Primary concern for production; people secondary
2. **1, 9 style.** Primary concern for people; production secondary
3. **1, 1 style.** Minimal concern for either production or people

[20] Robert R. Blake and Jane Srygley Mouton, "Management by Grid Principles of Situationalism," *Group & Organization Studies* (December 1981).
[21] Robert R. Blake and Jane Srygley Mouton, "A Comparative Analysis of Situationalism and 9,9 Management by Principle," *Organizational Dynamics* (Spring 1982).

4. **5, 5 style.** Moderate concern for both production and people to maintain the status quo
5. **9, 9 style.** High concern for both production and people as evidenced by personal commitment, mutual trust, and teamwork

Most managers prefer the 9,9 style, regardless of the situation at hand, since this style correlates positively with better results, better mental and physical health, and effective conflict resolution.

(C) Situational Leadership Theory Situational theory or contingency thinking is based on the assumption that successful leadership occurs when the leader's style matches the situation. It stresses the need for flexibility and rejects the notion of a universally applicable style.

BEHAVIORAL STYLES THEORY VERSUS SITUATIONAL THEORY

- Behavioral style theorists believe that there is one best style of leadership.
- Situational theorists are convinced that no one best style of leadership exists.

Different approaches to situational leadership include: Fred Fiedler's contingency theory, the path-goal theory, and the Vroom-Yetton-Jago decision-making model, as shown in Exhibit 5.56.

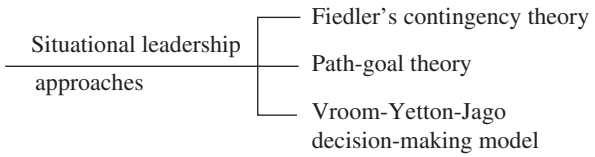


EXHIBIT 5.56 Situational Leadership Approaches

Fiedler's contingency theory, which has been thoroughly tested, is based on two assumptions. The performance of a leader depends on two interrelated factors: (1) the degree to which the situation gives the leader control and influence to accomplish the job, and (2) the leader's basic motivation: whether to accomplish the task or having close supportive relations with others (task-motivated leader has a concern for production and relationship-motivated leader has a concern for people).

WAYS TO ENHANCE WORKER MOTIVATION

Worker motivation can be increased by increasing the number and kinds of personal payoffs for achieving work goals. Other ways to increase worker motivation involve making paths to these payoffs easier to travel by clarifying the paths, reducing roadblocks and pitfalls, and increasing the opportunities for personal satisfaction en route.

Fiedler and his colleagues summed up their findings by noting that "everything points to the conclusion that there is no such thing as an ideal leader." Instead, *there are leaders, and there are situations.* The challenge to a manager is to analyze a leader's basic motivation and then match that leader with a suitable situation to form a product in combination. Fiedler believed that it is more efficient to move leaders to a suitable situation than to tamper with their personalities by trying to get task-motivated leaders to become relationship-motivated ones, or vice versa.

The **path-goal theory**, which is a derivative of expectancy motivation theory, emphasizes that leaders should motivate their followers by providing clear goals and meaningful incentives for reaching them. *Motivation is seen as essential to effective leadership.*

Path-goal proponents believe that managers need to rely contingently on four different leadership styles since personal characteristics of subordinates, environmental pressures, and work demands on subordinates will all vary from situation to situation. These four leadership styles include: directive (tell people what to do), supportive (treat subordinates as equals), participative (consult with subordinates), and achievement-oriented (set challenging goals). For example, a directive situational leadership style would be appropriate for a subordinate who possesses very low task maturity for a particular assignment.

PATH-GOAL THEORY VERSUS FIEDLER THEORY

- Path-goals theorists assume that managers can and do shift situationally from style to style.
- Fiedler theorists assume that managers cannot and do not change their basic leadership styles.

The Vroom-Yetton-Jago decision-making model. Vroom helped develop the expectancy theory of motivation based on the assumption that motivational strength is determined by perceived probabilities of success. The term "expectancy" refers to the subjective probabilities (or expectancy) that one thing will lead to another. Researchers Vroom, Yetton, and Jago (the Vroom model) portray leadership as a decision-making process with five distinct decision-making styles, each of which requires a different degree of subordinates' participation. The Vroom model qualifies as a situational-leadership theory because it prescribes different decision styles for varying situations managers typically encounter.

Of these five decision-making styles, two are autocratic, two are consultative, and one is group directed (see Exhibit 5.57). In addition, the Vroom model gives managers the tools for matching styles with various individual and group situations.

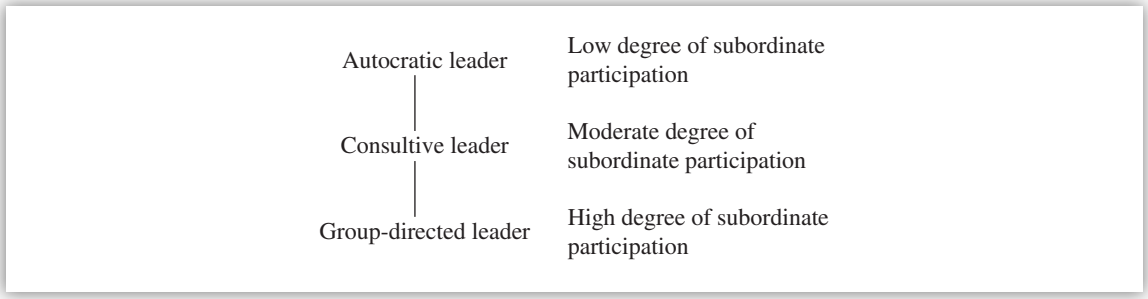


EXHIBIT 5.57 Decision-Making Styles

(D) Transformational Leadership Theory Transformational leaders are characterized as visionaries who challenge people to achieve exceptionally high levels of morality, motivation, and performance. Transformational leaders are masters of change, have charisma, rely on referent power, and can envision a better future, effectively communicate that vision, and get others to willingly make it a reality.

There is a distinction between a transactional leader and a transformational leader. Transactional leaders monitor people so they do the expected, according to plan (i.e., maintain status quo). In contrast, transformational leaders inspire people to do the unexpected, above and beyond the plan (fostering creative and productive growth).

TRANSACTIONAL LEADER VERSUS TRANSFORMATIONAL LEADERS

- Transactional leaders can best handle stable situations.
- Transformational leaders can best handle rapidly changing situations.
- Transformational theory combines the behavioral style theory and situational theory. Charismatic behavior is added to the traditional behavior.
- Laboratory and field research evidence generally supports the transformational leadership pattern.
- Followers of transformational leaders tend to perform better and to report greater satisfaction than those of transactional leaders.

(v) Leadership Categories

Leadership is of two categories: (1) good and bad leaders and (2) formal and informal leaders. Effective leadership is associated with both better performance and more ethical performance. According to Chester Schriesheim, James Tolliver, and Orlando Behling,[22] leadership is "a social influence process in which the leader seeks the voluntary participation of subordinates in an effort to reach organizational objectives." Exhibit 5.58 provides a comparison between formal and informal leadership.

Formal leadership	Informal leadership
Formal leadership is the process of influencing relevant others to pursue official organizational objectives.	Informal leadership is the process of influencing others to pursue unofficial objectives that may or may not serve the organization's interests
Formal leaders have a measure of legitimate power because of their formal authority.	Informal leaders lack formal authority.
Formal leaders rely on an expedient combination of reward, coercive, referent, and expert power.	Informal leaders rely on an expedient combination of reward, coercive, referent, and expert power.
Formal leaders can be an asset or a liability to the organization (asset when they work for the organization; liability when they work against the organization).	Informal leaders can be an asset or a liability to the organization (asset when they work for the organization; liability when they work against the organization).

EXHIBIT 5.58 Comparison of Formal Leadership with Informal Leadership

Power is needed in all organizations. Power must be used because managers must influence those they depend on. It is powerlessness, not power, that undermines organizational effectiveness.

Power is the ability to manage all types of resources to accomplish something of value to the organization. These resources could be human, material, and informational in content. Power

[22] Chester Schriesheim, James Tolliver, and Orlando Behling, "Influence Tactics Used by Subordinates," *Journal of Applied Psychology* (June 1990).

affects organizational members in three areas: decision making, behavior, and situations. Another dimension to power is to distinguish between "power over" (ability to dominate), "power to" (ability to act freely), and "power from" (ability to resist the demands of others).

AUTHORITY VERSUS POWER

- Authority is the right to direct the activities of others. It is an officially sanctioned privilege that may or may not get results.
- Power is the demonstrated ability to get results.
- One may alternatively possess authority but have no power, possess no authority yet have power, or possess both authority and power.
- A manager who gets subordinates to work hard on an important project has both authority and power.

Experts on power say that power is neutral. It is a tool that can be used in a positive or negative manner. Power exercised for power's sake can be quite dangerous to all parties affected. The five bases of power exhibited by leaders are listed next.

1. **Reward power** is gaining compliance through rewards.
2. **Coercive power** is gaining compliance through fear or threat of punishment.
3. **Legitimate power** is compliance based on one's formal position and parallels formal authority (job title). It can be eroded by its frequent abuse (or overuse).
4. **Referent power** is compliance based on charisma, personal identification, or attraction and has no relation to job title.
5. **Expert power** is compliance based on the ability to dispense valued information and is based on the knowledge or skills possessed by a person.

(vi) Mentoring

Mentoring is a relationship in which experienced managers aid employees in the earlier stages of their careers. Such a relationship provides an environment for conveying technical, interpersonal, and organizational skills from the more-experienced to the less-experienced person. Not only does the inexperienced employee benefit, but the mentor may enjoy the challenge of sharing wisdom and knowledge.

However, mentoring has problems. Young minority managers frequently report difficulty in finding mentors. Also, men generally show less willingness than women do to be mentors. Further, mentors who are dissatisfied with their jobs and those who teach a narrow or distorted view of events may not help a young manager's development. Fortunately, many managers have a series of advisors or mentors during their careers and may find advantages in learning from the different mentors. For example, the unique qualities of individual mentors may help less-experienced managers identify key behaviors in management success and failure. Further, those being mentored find previous mentors to be useful sources for networking.

(vii) Delegation

Delegation is the process of assigning various degrees of decision-making authority to subordinates. It is not an all-or-nothing proposition. Authority may be passed along to subordinates; ultimate

responsibility cannot be passed along. Thus delegation is the sharing of authority, not the abdication of responsibility. Experts say that it is good to delegate those activities the manager knows best.

Advantages from Delegation

- Managers can free more of their time for planning and motivating.
- Subordinates will be better trained and developed as future managers (e.g., acting as audit liaison on special task force to develop promising audit subordinates).

Barriers to Delegation

- Lack of confidence and trust in subordinates
- Vague job definition
- Fear of competition from subordinates
- Poor example set by superiors who do not delegate
- Reluctance in taking the risks involved in depending on others

For example, an internal auditing manager can delegate the following tasks to a senior auditor with potential for promotion to manager:

- Conducting a scheduled entrance conference for an upcoming audit
- Reviewing the working papers of an audit that is nearing completion
- Developing a staff assignment schedule for the next quarter

But the auditor manager cannot delegate an initiating action on the board of directors' request to look at the company's pension plans since the senior auditor is not ready and the board's request is high level, which means it requires experience and maturity.

(b) Group Synergy through Team Building

(i) Role of Worker as Individual or Team Member

Every worker has a dual role: as an individual and as a member of a group. A **group** is defined by functional qualities, not physical properties.[23] A group consists of a minimum of two or more people who interact, communicate with, and influence each other for a period of time. To comprise a group, a collection of people must share more than circumstances. They must share perceptions and goals. Group members must be aware of each other, interact with each other, and exert influence on each other. To communicate with each other, they must both send and receive messages. And they must be engaged in these processes for more than a few moments.

Why do people join groups? Formal or otherwise, there are two common reasons why people join groups: goal attainment and needs gratification. By working together, people can accomplish goals that might be difficult or impossible for solitary individuals to achieve. Additionally, group participation addresses many social needs such as access to approval, a sense of belonging, friendship, and love.

(A) Individuals in Group Context People do not inevitably lose their individuality in groups, although groups may help lessen self-awareness and produce a state of deindividuation. In fact, group

[23] Ann L. Weber, *Social Psychology* (New York: HarperCollins, 1992).

membership can heighten certain aspects of individual experience. Three important effects of the group on the individual are identity, deviance, and social impact (see Exhibit 5.59).

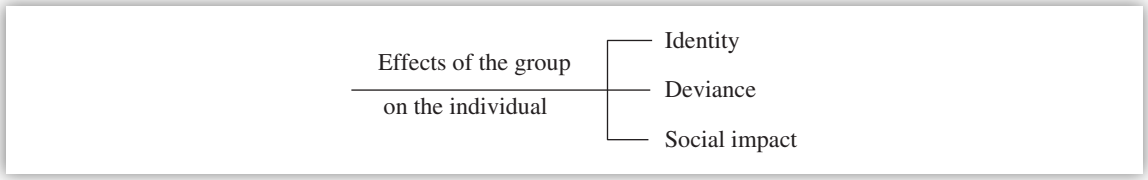


EXHIBIT 5.59 Effects of the Group on the Individual

- **Identity.** Belonging to a group is a form of social categorization: The group becomes one aspect of social identity (e.g., a member of IIA). Reference groups are particularly important in defining not only identity but also aspirations. A reference group is a social network one consults for social comparison. When groups come into contact with each other, individuals may compare their own group favorably to the alternatives available.
- **Deviance.** Group goals sometimes can override or conflict with individual member's personal goals. When a member breaks with the group's norms to satisfy personal needs, he or she becomes a deviant. Members of a group are important in validating each other's beliefs. A deviant threatens that validation by defecting and reducing consensus. Ultimately the deviant will most likely be pushed out of the group, thus restoring consensus with one fewer member.
- **Social impact.** Social impact theory is an explanation of social influence. According to this theory, the degree to which a targeted individual is influenced depends on three factors: the strength of the source of influence, the immediacy of the influence, and the number of sources. Group membership can be seen as having social impact on an individual. Taken factor by factor, a group will have greater influence on each member if it is strong, if the group's influence is immediate, and if the group is large in number.

(B) Group Structures Groups have tasks such as solving problems and making decisions (task agenda) and meeting the emotional needs and social roles of the group's members (social agenda). Groups meet these two agendas through several key processes and structures: norms, roles, and cohesiveness (see Exhibit 5.60).

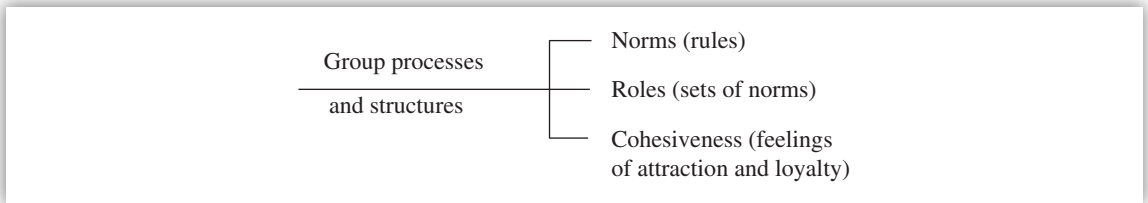


EXHIBIT 5.60 Group Processes and Structures

Norms are rules or guidelines for accepted and expected behavior. Some norms are explicit; members know what they are and can explain them to newcomers. Others are implicit or subtle, occasionally taken for granted until a deviation occurs. Most groups have a norm for how decisions are made. For example, a group of coworkers in a small business may agree that important contracts are to be voted on by all members, with a simple majority of more than half ruling. The coworker who tries to play dictator will be violating norms and may be treated as a deviant until the group restores consensus or pushes the deviant out.

Roles are sets of norms defining appropriate behaviors. Groups usually involve roles; some are broad (leaders and followers), while others are more specific. Roles differentiate members' functions and contributions within the group. Roles may be organized according to individual talents. Roles can be a source of reward as well as a source of problems within a group. Group membership offers personal benefits, and group participation achieves goals that solitary individuals may not.

Roles may differ not only in function but also in value to the group. Values are abstract ideas that shape an individual's thinking and behavior. Roles associated with greater prestige or respect are said to have higher-status position or rank. Status affects the way members of the group communicate and work with each other. For example, high-status members, such as bosses and managers, may initiate communication with lower-status members, but not vice versa. A manager can interrupt a subordinate worker to ask a question, but a subordinate worker is not free to enter a manager's office and ask questions without permission. Status can be a reward for specific members, but it carries a cost, since differences in status can be a source of resentment or competition among members.

Two kinds of role conflict commonly occur: person–role conflict and interrole conflict. Person–role conflict is where a person finds his or her group role difficult to perform. For example, a committee member may be required to criticize other members' work but might feel uncomfortable with having to do this.

Interrole conflict is where members in different groups compete with each other. For example, a church member may feel conflicted when her company schedules a workshop on a date with church significance. To be a good church member, she should skip the workshop; to be a good employee, she must violate church standards. Interrole conflict can be a familiar—if not minor—problem.

When a person's responsibilities within a group are unclear or unstable, the individual suffers the difficulty of role ambiguity. Roles are likely to be ambiguous when a member first joins a group or when task performance changes. For example, if a small service company shifts from paper record keeping to the use of computers, the roles of the file clerk may become ambiguous. It is not yet clear what—if any—function he will have in the organization from this point on.

Cohesiveness is a feeling of attraction and loyalty that motivates members to stay in the group. Members of cohesive groups like each other more and support common goals more strongly than members of less cohesive groups. High cohesiveness can be a source of both benefits and liabilities. Members of highly cohesive groups enjoy their membership and interaction more but are also prone to make mistakes by giving group feeling a higher priority than other group goals.

Anything that makes a group more valuable to its members increases cohesiveness. Competition within the group can reduce cohesiveness, since members fear threats from each other. Another barrier to fellowship is disliking or special preferences among members. When members are drawn to and away from each other, subgroups form, which break down organizational unity. Preferential differences in members' feelings are more likely to develop in large groups, and thus group size is negatively related to cohesiveness; the larger the organization, the harder it is to maintain attraction, loyalty, and fairness evenly among all members.

(ii) Methods Used in Team Building

After a team has been created, there are distinct stages through which it develops. New teams are different from mature teams. Recall a time when you were a member of a new team, such as a

fraternity or sorority pledge class, a committee, or a small team formed to do a class assignment. Over time, the team changed. In the beginning, team members had to get to know one another, establish roles and norms, divide the labor, and clarify the team's task. In this way, members became parts of a smoothly operating team. The challenge for leaders is to understand the stage of the team's development and take action that will help the group improve its functioning.

Research findings suggest that team development is not random but evolves over definitive stages. One useful model for describing these stages contains five phases:

1. Forming
2. Storming
3. Norming
4. Performing
5. Adjourning

The **forming** stage of development is a period of orientation and getting acquainted. Members break the ice and test one another for friendship possibilities and task orientation. Team members find which behaviors are acceptable to others. Uncertainty is high during this stage, and members usually accept whatever power or authority is offered by either formal or informal leaders. Members are dependent on the team until they find out what the ground rules are and what is expected of them. During this initial stage, members are concerned about such things as "What is expected of me?" "What is acceptable?" and "Will I fit in?" During the forming stage, the team leader should provide time for members to get acquainted with one another and encourage them to engage in informal social discussions.

During the **storming** stage, individual personalities emerge. People become more assertive in clarifying their roles and what is expected of them. Conflict and disagreement mark this stage. People may disagree over their perceptions of the team's mission. Members may jockey for positions, and coalitions or subgroups based on common interests may form. One subgroup may disagree with another over the total team's goals or how to achieve them. The team is not yet cohesive and may be characterized by a general lack of unity. Unless teams can move beyond this stage, they may get bogged down and never achieve high performance. During the storming stage, the team leader should encourage participation by each team member. Members should propose ideas, disagree with one another, and work through the uncertainties and conflicting perceptions about team tasks and goals.

During the **norming** stage, conflict is resolved, and team harmony and unity emerge. Consensus develops on who has the power, who is the leader, and members' roles. Members come to accept and understand one another. Differences are resolved, and members develop a sense of team cohesion. This stage typically is of short duration. During the norming stage, the team leader should emphasize oneness within the team and help clarify team norms and values.

During the **performing** stage, the major emphasis is on problem solving and accomplishing the assigned task. Members are committed to the team's mission. They are coordinated with one another and handle disagreements in a mature way. They confront and resolve problems in the interest of task accomplishment. They interact frequently and direct discussion and influence toward achieving team goals. During this stage, the leader should concentrate on managing high task performance. Both socioemotional and task specialists should contribute.

The **adjourning** stage occurs in committees, task forces, and teams that have a limited task to perform and are disbanded afterward. During this stage, the emphasis is on wrapping up and gearing down. Task performance is no longer a top priority. Members may feel heightened emotionality, strong cohesiveness, and depression or even regret over the team's disbandment. They may feel happy about mission accomplishment and sad about the loss of friendship and associations. At this point, the leader may wish to signify the team's disbanding with a ritual or ceremony, perhaps giving out plaques and awards to signify closure and completeness.

The five stages of team development typically occur in sequence. In teams that are under time pressure or that will exist for only a short period of time, the stages may occur quite rapidly. The stages may also be accelerated for virtual teams. For example, bringing people together for a couple of days of team building can help virtual teams move rapidly through the forming and storming stages.

(iii) Assessing Team Performance

Another important aspect of the team process is cohesiveness. **Team cohesiveness** is defined as the extent to which members are attracted to the team and motivated to remain in it. Members of highly cohesive teams are committed to team activities, attend meetings, and are happy when the team succeeds. Members of less cohesive teams are less concerned about the team's welfare. High cohesiveness is normally considered an attractive feature of teams.

Characteristics of team structure and context influence cohesiveness. First is **team interaction**. The greater the contact among team members and the more time spent together, the more cohesive the team. Through frequent interactions, members get to know one another and become more devoted to the team. Second is the concept of **shared goals**. If team members agree on goals, they will be more cohesive. Agreeing on purpose and direction binds the team together. Third is **personal attraction to the team**, meaning that members have similar attitudes and values and enjoy being together.

Two factors in the team's context also influence group cohesiveness. The first is the presence of competition. When a team is in moderate competition with other teams, its cohesiveness increases as it strives to win. Finally, team success and the favorable evaluation of the team by outsiders add to cohesiveness. When a team succeeds in its task and others in the organization recognize the success, members feel good, and their commitment to the team will be high.

The outcome of team cohesiveness can fall into two categories: morale and productivity. As a general rule, morale is higher in cohesive teams because of increased communication among members, a friendly team climate, maintenance of membership because of commitment to the team, loyalty, and member participation in team decisions and activities. High cohesiveness has almost uniformly good effects on the satisfaction and morale of team members.

With respect to team performance, research findings are mixed, but cohesiveness may have several effects. First, in a cohesive team, members' productivity tends to be more uniform. Productivity differences among members are small because the team exerts pressure toward conformity. Noncohesive teams do not have this control over member behavior and therefore tend to have wider variation in member productivity.

With respect to the productivity of the team as a whole, research findings suggest that cohesive teams have the potential to be productive, but the degree of productivity depends on the

relationship between management and the working team. Thus, team cohesiveness does not necessarily lead to higher team productivity. One study surveyed more than 200 work teams and correlated job performance with their cohesiveness. Highly cohesive teams were more productive when team members felt management support and less productive when they sensed management hostility and negativism. Management hostility led to team norms and goals of low performance, and the highly cohesive teams performed poorly, in accordance with their norms and goals.

HOW MANY TEAMS ARE THERE?

In most organizations, employees work in teams to achieve goals. Many types of teams can exist within organizations. The easiest way to classify teams is in terms of those created as part of the organization's formal structure and those created to increase employee participation. Examples include formal teams, vertical teams, horizontal teams, virtual teams, global teams, special-purpose teams, problem-solving teams, self-directed teams, self-managing teams, and committees.

- **Formal teams** are created by the organization as part of the formal organization structure. Two common types of formal teams are vertical and horizontal, which typically represent vertical and horizontal structural relationships.
- A **vertical team** is composed of a manager and his or her subordinates in the formal chain of command. Sometimes called a *functional team* or a *command team,* the vertical team may in some cases include three or four levels of hierarchy within a functional department. Typically, the vertical team includes a single department in an organization. The third-shift nursing team on the second floor of St. Luke's Hospital is a vertical team that includes nurses and a supervisor. A financial analysis department, a quality control department, an accounting department, and a HR department are all command teams. Each is created by the organization to attain specific goals through members' joint activities and interactions.
- A **horizontal team** is composed of employees from about the same hierarchical level but from different areas of expertise. A horizontal team is drawn from several departments, is given a specific task, and may be disbanded after the task is completed. The two most common types of horizontal teams are task forces and committees.

  As part of the horizontal structure of the organization, task forces and committees offer several advantages:

  - They allow organization members to exchange information.
  - They generate suggestions for coordinating the organizational units that are represented.
  - They develop new ideas and solutions for existing organizational problems.
  - They assist in the development of new organizational practices and policies.
- A **virtual team** is made up of geographically or organizationally dispersed members who are linked primarily through advanced information and telecommunications technologies. Although some virtual teams may be made up of only organizational members, virtual teams often include contingent workers, members of partner organizations, customers, suppliers, consultants, or other outsiders. Team members use e-mail, voice mail, videoconferencing, Internet and intranet technologies, and various types of collaboration software to perform their work, although they may also sometimes meet face to face.

  Virtual teams are highly flexible and dynamic. Some are temporary cross-functional teams pulled together to work on specific projects or problems while others are long-term or permanent self-directed teams.

  Team leadership typically is shared or altered, depending on the area of expertise needed at each stage of the project. In addition, team membership in virtual teams may change fairly quickly,

depending on the tasks to be performed. One of the primary advantages of virtual teams is the ability to rapidly assemble the most appropriate group of people to complete a complex project, solve a particular problem, or exploit a specific strategic opportunity. The success of virtual teams depends on several factors, including selecting the right members, building trust, sharing information, and effectively using technology. For example, VeriFone Company uses virtual teams in every aspect of its business. Virtual teams are also called global teams.

- **Global teams** are cross-border work teams made up of members of different nationalities whose activities span multiple countries. Generally, global teams fall into two categories: intercultural teams, whose members come from different countries or cultures and meet face to face, and virtual global teams, whose members remain in separate locations around the world and conduct their work electronically.

  Global teams can present enormous challenges for team leaders who have to bridge gaps of time, distance, and culture. In some cases, members speak different languages; use different technologies; and have different beliefs about authority, time orientation, decision making, and so forth. Culture differences can significantly affect teamwork and relationships. Organizations using global teams invest the time and resources to adequately educate employees. They have to make sure all team members appreciate and understand cultural differences, are focused on goals, and understand their responsibilities to the team. For a global team to be effective, all team members must be willing to deviate somewhat from their own values and norms and establish new norms for the team. As with virtual teams, carefully selecting team members, building trust, and sharing information are critical to success.

- **Special-purpose teams,** sometimes called *project teams*, are created outside the formal organization structure to undertake a project of special importance or creativity. Special-purpose teams focus on a specific purpose and expect to disband once the specific project is completed.

- **Problem-solving teams** typically consist of 5 to 12 hourly employees from the same department who voluntarily meet to discuss ways of improving quality, efficiency, and the work environment. Recommendations are proposed to management for approval. Problem-solving teams usually are the first step in a company's move toward greater employee participation. The most widely known application is quality circles, initiated by Japanese companies, in which employees focus on ways to improve quality in the production process.

- **Self-directed teams.** Employee involvement through teams is designed to increase the participation of low-level workers in decision making and the conduct of their jobs, with the goal of improving performance. Employee involvement started out simply with techniques such as information sharing with employees or asking employees for suggestions about improving the work. Gradually, companies moved toward greater autonomy for employees, which led first to problem-solving teams and then to self-directed teams.

  As a company matures, problem-solving teams gradually can evolve into self-directed teams, which represent a fundamental change in how employee work is organized. Self-directed teams enable employees to feel challenged, find their work meaningful, and develop a strong sense of identity with the company. Self-directed teams typically consist of 5 to 20 multiskilled workers who rotate jobs to produce an entire product or service or at least one complete aspect or portion of a product or service (e.g., engine assembly, insurance claim processing). The central idea is that the teams themselves, rather than managers or supervisors, take responsibility for their work, make decisions, monitor their own performance, and alter their work behavior as needed to solve problems, meet goals, and adapt to changing conditions. Characteristics of these self-directed teams, which are permanent teams, are listed next.

  - The team includes employees with several skills and functions, and the combined skills are sufficient to perform a major organizational task. A team may include members from the foundry, machining, grinding, fabrication, and sales departments, with members cross-trained to perform one another's jobs. The team eliminates barriers among departments, enabling excellent coordination to produce a product or service.

- The team is given access to resources such as information, equipment, machinery, and supplies needed to perform the complete task.
- The team is empowered with decision-making authority, which means that members have the freedom to select new members, solve problems, spend money, monitor results, and plan for the future.

In a self-directed team, team members take over managerial duties such as scheduling or ordering materials. They work with minimum supervision, perhaps electing one of their own as supervisor, who may change each year. The most effective self-directed teams are those that are fully empowered. In addition to having increased responsibility and discretion, empowered teams are those that have a strong belief in their team's capabilities; find value and meaning in their work; and recognize the impact the team's work has on customers, other stakeholders, and organizational success. Managers create the conditions that determine whether self-directed teams are empowered by giving teams true power and freedom, complete information, knowledge and skills, and appropriate rewards.

- **Self-managing teams.** The scope of self-managing teams includes not only the normal work routine but also some of the traditional managerial tasks. Employees are assigned to self-managed teams. Team members get rotated for cross-training purposes. The manager's role becomes more of a facilitator rather than the traditional supervisor role.

  Teamwork is the key strategy to improving productivity, because all improvements involve people implementing change in a system. A system is a combination of social and technical systems. Management researchers say that better social systems, even at the expense of the technical systems, yield better results. The optimal social system is the self-managing team concept. It consists of a series of work teams consisting of 5 to 10 members who rotate jobs and produce an entire product or service with minimal supervision. The team assumes all responsibilities and makes all decisions regarding their product or service.

  Self-managing teams have been extremely effective, because they challenge all workers to actively and mentally participate rather than blindly execute policies. This results in continuous productivity and quality improvements, and ultimately success. Meaningful participation by workers always will have a positive impact on productivity. Empowering workers to do those things that enable them to work smarter is a powerful tool in increasing productivity.

- **Committees.** People join various groups or committees to reach decisions and solve problems. An ad hoc committee is formed for a short period with a specific purpose and is disbanded after the purpose is accomplished. The members of the ad hoc committee will come from functional departments, such as manufacturing, HR, law, and marketing.

  A steering committee is a long-term group of people focusing on a specific area of an organization such as information systems and new product development. A standing committee exists indefinitely. A focus group is put together for the purpose of analyzing and researching various public issues for the betterment of citizens. This group consists of private citizens.

  When committees are used in the decision-making process, a manager may use one of two formats: group-aided or group decision making. In the first instance, the group does everything but make the final decision; the manager makes the final decision. In the second instance, the group actually makes the decision. One of the advantages of group-aided decision making over group decision making is that personal accountability for the decision is maintained. In "group" decision making, the fact that the decision was made by a committee obscures the role of personal accountability.

  An example of a group-aided decision-making scenario in internal audit follows. The general auditor of a company is attempting to standardize the audit procedures used throughout the company. Many of the auditors are employed at distant locations. The general auditor wants to select a process that will encourage input from a cross section of auditors, facilitate differing perspectives, and encourage acceptance of the changes that might result from the standardization.

A committee generally is long-lived and may be a permanent part of the organization's structure. Membership on a committee usually is decided by a person's title or position rather than by personal expertise. A committee often needs official representation, compared with selection for a task force, which is based on personal qualifications for solving a problem. Committees typically are formed to deal with tasks that recur regularly. For example, a grievance committee handles employee grievances; an advisory committee makes recommendations in the areas of employee compensation and work practices; a worker–management committee may be concerned with work rules, job design changes, and suggestions for work improvement.

5.4 Conflict Management

Topics such as negotiation skills, conflict types and their resolution methods, and added-value negotiating concepts are discussed in this section.

(a) Negotiating Skills

Negotiation is a decision-making process among different parties with different preferences. Two common types of negotiation include two party (buyer and seller) and third party (buyer, seller, and agent). Traditionally, negotiation takes a win–lose attitude, which is based on power, position, and competition. Here, one person's success is achieved at the expense of the success of others. It takes something from the other party. However, win–win attitude is based on high principles and cooperativeness among parties. Here, one person's success is not achieved at the expense of the success of others. Every party gets something.

(i) Process of Negotiation

A negotiation is more than an exchange of material objects and words.[24] It is a way of acting and behaving that can foster understanding, belief, acceptance, respect, and trust between two or more parties. It is the manner of your approach, the tone of your voice, the attitude you convey, the methods you use, and the concern you exhibit for the other side's feelings and needs. All these things comprise the process of negotiation. Hence, the way you go about trying to achieve your objective may, in and of itself, meet some of the other party's needs.

A conflict situation is the prerequisite to negotiation. Conflict is an unavoidable part of life. It occurs when the goals of each party are in opposition. But conflict can arise even if both parties are in agreement about what they want—sometimes the conflict may be centered around how to get it (or the means used). Conflict may arise from differences in experiences, information, or attitudes about the different roles of the negotiators.

(A) Why Opposition? Opposition is essential because it results in growth and progress. People who are dissatisfied with the status quo generate tension with their different ideas, which often leads to a creative solution. Thus, opposition is the foundation of progress and growth.

(B) What Is Negotiation? Negotiation is gaining the favor of people from whom we want things, such as money, justice, status, and recognition. People with technical experience, such as accountants

[24] Herb Cohen, *You Can Negotiate Anything* (Secaucus, NJ: Lyle Stuart, 1980).

and auditors, are often frustrated because they lack the negotiating skills needed to sell their ideas and audit findings to auditees and management alike. Auditors also need negotiating skills to obtain help from and support of colleagues, supervisors, peers, auditees, and even friends and family members.

(C) Elements of Negotiation Three crucial elements exist in a negotiation: power, time, and information. People can negotiate anything with these three tightly interrelated variables.

1. **Power.** The other side always seems to have more power and authority than you think you have.
2. **Time.** The other side does not seem to be under the same kind of organizational pressure and time constraints you feel you are under.
3. **Information.** The other side seems to know more about you and your needs than you know about them and their needs.

Negotiating is analyzing information, time, and power to affect people's behavior—it is the meeting of two or more parties in order to make things happen to their mutual satisfaction.

A simple test to make sure that you are ready for negotiation is to ask the following three questions. A "yes" answer will indicate readiness.

1. Am I comfortable negotiating in this particular situation?
2. Will negotiating meet my needs?
3. Is the expenditure of energy and time on my part worth the benefits that I can receive as a result of this encounter?

Power Power comes in many forms and is exercised in many ways. Power is the capacity or ability to get things done, to exercise control over people, events, situation, or oneself. Power enables you to change your reality to achieve your goal. Power could imply a master–slave relationship, with one side dominating the other. It is also true that some people misuse power or employ it in a manipulative way. *People, especially auditors, should be reality oriented—they must learn to see things as they really are without passing judgment.*

Power is neutral. It is a means, not an end. Power, like beauty, is strictly in the eye of the beholder. Most people have more power than they realize. Even the *perception* that one party might help or hurt the other party can provide power in the relationship. The reality of the situation is immaterial.

The power of identification plays a significant role in negotiations and decision making. It is the ability of getting others to identify with you. Although you must be persistent and tenacious when negotiating, behaving decently and trying to help others goes a long way in negotiations. Logic, in and of itself, will rarely influence people. Most often logic does not work. If you want to persuade people, show the immediate relevance, benefits, and value of what you are saying in terms of meeting their needs and desires. *In all negotiations, there is an element of risk, that is, uncertainty about the outcome of negotiation.*

Getting the commitment of team members in a project is a must for effective negotiation. *Involvement begets commitment. Commitment begets power.* People usually respect the power of expertise in a person with technical knowledge, a specialized skill, or better experience than they have.

There is a direct ratio between the extent of an investment and the willingness to compromise. The more investment in time, effort, or money is made, the quicker the compromise usually can be reached.

Time The passage of time affects the negotiation process. Time can favor either side, depending on the circumstances. It pays to be patient since most concession behavior and settlements will occur at or even beyond the deadline. Remain calm, but keep alert for the favorable moment to act. In an adversarial negotiation, the best strategy is not to let the other side know the real deadline.

The best outcome in negotiations comes only slowly. As the deadline approaches, creative solutions or turnaround situations by the other side occur. The people may not change but, with the passage of time, circumstances do.

Information Information is power, especially when negotiating with a party that cannot be fully trusted. The idea is that the more information you have about the other party's priorities, constraints, costs, real needs, and organizational pressures, the better you will be able to bargain.

Effective listening techniques really help during negotiations. Just by listening, you can learn a great deal about the other side's feelings, motivations, and real needs. Attentive listening means understanding what is being omitted, not just hearing what is being said. When you begin to hear generalities, it is a signal to start asking specific questions for clarification purposes.

Auditors must be cognizant of behavioral cues. A **cue** is a message sent indirectly; its meaning may be ambiguous and may require interpretation. Three basic categories of cues exist.

1. **Unintentional cues**, in which behavior or words transmit an inadvertent message (e.g., slip of the tongue).
2. **Verbal cues**, in which voice intonation or emphasis sends a message that seems to contradict the words being spoken.
3. **Behavioral cues**, which are the language of the body as displayed by posture, facial expressions, eye contact (or lack thereof), hand gestures, raised eyebrows, a smile, a touch, a wink, or a scowl. You must be sensitive to the nonverbal factors (behavioral cues) in any communication.

It is important to listen with your "third ear," observe with your "third eye," and detach yourself from the meeting so that you can hear the words in their proper nonverbal context. During negotiations or communications, cues are meaningful if they are part of a cluster and indicate the direction of movement.

(D) Modes of Negotiations Two modes of negotiating behavior/conflict resolution exist: the competitive strategy and the collaborative (cooperative) strategy. The style of negotiators can range between these two strategies (see Exhibit 5.61).

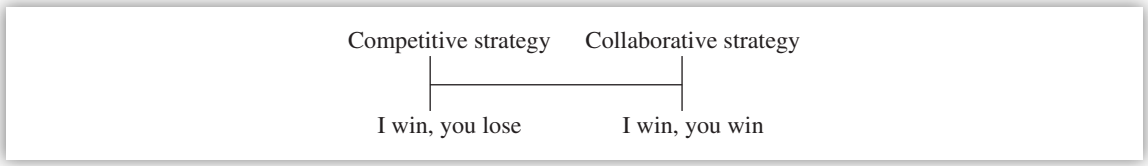


EXHIBIT 5.61 Style of Negotiators

Competitive strategy focuses on getting what you want and defeating an opponent (I win, you lose). This may range from intimidation to manipulation. People applying competitive strategy often start with tough demands, get red-faced, raise their voices, act exasperated, delay making any concession, tend to be patient, and ignore deadlines.

When the other party is focusing on competitive strategy, it is better to switch to collaborative (cooperative) strategy. Collaborative strategy shifts the effort from trying to defeat an opponent to trying to defeat a problem and to achieve a mutually accepted outcome. With this method, all parties work together to find an acceptable solution or common ground that will meet the needs of both sides.

The best way to start a collaborative strategy is to say something like "I need your help with this problem" or to employ tact and exhibit concern for the other's dignity. Even if the other party has a reputation for being obnoxious, negative, and contrary, he or she will be disarmed by an approach that conveys positive expectations. If given a chance, most people try to be accommodating and play the role suggested for them. In other words, *people tend to behave the way you expect them to behave.*

Try to see the problem from the other party's point of view or frame of reference. Listen with empathy, which means stop working on counterarguments while others are speaking. The trick is not to be abrasive because *how* you say something will determine the response you get. Avoid using absolutes when responding to the other party's offer.

When people see themselves as adversaries, they deal at arm's length. From this distance they state demands and counterdemands, pronounce conclusions, and give ultimatums to each other. Since each party attempts to increase its relative power, significant data, facts, and information are hoarded. Each party conceals feelings, attitudes, and real needs. Obviously, in such a climate, it is virtually impossible to negotiate for the satisfaction of mutual needs.

Accomplishing mutual satisfaction using the collaborative win-win style involves emphasis on three important activities:

1. Building trust
2. Gaining commitment
3. Managing opposition

Building trust requires a firm belief in the honesty and reliability of the other party. It is a mutual dependence—a potential alliance that allows both sides to deal with inevitable disagreement. It is a climate that lays the foundation for transforming conflict into satisfying outcomes. This mutual trust is the mainspring of collaborative win-win negotiations. *It is a fact of life that no one will ever tell you anything worthwhile unless you are trusted with that information.*

In collaborative negotiations, there is no need for conniving, intimidating, fast-talking, manipulating, or wheeling and dealing. Trusting each other creates a climate of confidence where the needs of both sides can be fully satisfied and their positions enhanced. When parties distrust one another, it can lead to hostility and destructive negotiations. Auditors, in particular, should take note of this statement: Often they are distrusted by auditees.

Gaining the commitment of people who support your idea will do wonders. Never see anyone as an isolated entity or unit. Envision those whom you wish to persuade in context; see them as

a central core around which others move. Get the faith and backing of those other people and you will influence the position and movement of the core.

Dealing with or **managing the opposition** involves encouraging the pooling of ideas, information, and experience in order to find a mutually beneficial outcome. At all times, avoid any possible public embarrassment to the people with whom you are negotiating. Train yourself to speak honestly to idea opponents without offending them. Make your point and present your case without making the other party an enemy.

Winning means fulfilling your needs while being consistent with your beliefs and values. You can get what you want if you recognize that each person is unique and that his or her needs can be reconciled with your own. At the same time, never forget that most needs can be fulfilled by the way you act and behave. Mutual satisfaction should be your goal, and the means of achievement is the essence of collaborative win-win negotiations.

(E) Compromise versus Collaboration The word "compromise" is not synonymous with "collaboration." Compromise results in an agreement in which each side gives up something it really wanted. Compromise is an outcome where no one's needs are fully met. This is because the strategy of compromise rests on the faulty premise that your needs and the other party's needs are always in opposition. With this thinking, it is never possible for mutual satisfaction to be achieved. Each party starts out with greater (extreme) demands, hoping to compromise at a midpoint. This is not to say that compromise is always a poor choice. Often the strategy of compromise may be appropriate, depending on the particular circumstances.

Successful collaborative negotiations depend on finding out what the other side really wants and showing them a way to get it while still getting what you want. It is the definition of win-win. Auditors should practice successful collaborative negotiations to reach a win-win situation.

Dos of Negotiations

- Do use phrases such as "I don't know," or "I don't understand it," which can result in negotiating leverage.
- Do approach others and ask for help. It tends to set the climate for a mutually beneficial relationship. At the very least, you will cause the other side to make an investment that ultimately accrues to your advantage.

Don'ts of Negotiations

- Don't be too quick to "understand" or prove your intellect at the outset of an encounter. Learn to ask questions, even when you think you might know the answers.
- Never give an ultimatum at the beginning of a negotiation. An ultimatum must come at the end of a negotiation, if at all.
- Do not use "hard" ultimatums, such as "Take it or leave it" or "It is this way or else!" These attitudes are self-defeating. Use "soft" ultimatums, such as "Your position is valid, but this is all I can do at the moment. Help me."
- Never leave the other side without alternatives. Always allow them to make some kind of choice.
- Don't reduce the other side's stress unless you receive what you are shooting for.

- Don't be abrasive, because how you say something often determines the response you get.
- Avoid using absolutes when responding to people. Learn to preface your replies with "What I think I may have heard you say." This "lubricant demeanor" will soften your words, consecrate your actions, and minimize the friction.
- Avoid publicly embarrassing the people with whom you deal. Never ridicule anyone in front of others. Even when you are right, shun all opportunities to humiliate people, especially in public.
- Never forget the power of your attitude.
- Never judge the actions and motives of others.

(ii) Another Perspective on Negotiation

Fisher, Ury, and Patton, in their book *Getting to Yes: Negotiating Agreement without Giving In*,[25] discuss two types of negotiations: positional bargaining (least effective, least efficient, and least amicable) and principled negotiation (most effective, most efficient, and most amicable). Positional bargaining can be soft (on the people and the problem) or hard (on the people and the problem). The authors say that arguing over positions produces unwise agreements and endangers ongoing relationships. They suggest a principled negotiation, or negotiation on the merits, as an alternative to the traditional method of positional bargaining. Participants in the principled negotiation are problem solvers, and the goal is a wise outcome reached efficiently and amicably.

There are four key ingredients to principled negotiations:

1. **Separate the people from the problem (people).** The key thing to remember is to be soft on the people and hard on the problem.
2. **Focus on interests, not positions (interests).** The key things to remember are to explore interests and to avoid having a bottom line number.
3. **Generate options for mutual gain (options).** The key things to remember are to develop mutual options to choose from and decide later.
4. **Insist on using an objective standard (criteria).** The key things to remember are to try to reach a result based on standards independent of will; try to maintain reason and be open to reason; and yield to principle, not pressure.

Fisher, Ury, and Patton suggest that substantive issues, such as terms, conditions, prices, dates, numbers, and liabilities, should be disentangled from relationship issues, such as balance of emotion and reason, ease of communication, degree of trust and reliability, attitude of acceptance or rejection, relative emphasis on persuasion or coercion, or degree of mutual understanding.

There is no trade-off between pursuing a good substantive outcome and pursuing a good relationship outcome. A good working relationship tends to make it easier to get good substantive outcomes (for both sides). Good substantive outcomes tend to make a good relationship even better.

Each party (buyer and seller) in the negotiation process should have its own best alternative to a negotiating agreement (BATNA), which is a settlement amount (bottom line) if negotiations do

[25] Roger Fisher, William L. Ury, and Bruce Patton, *Getting to Yes: Negotiating Agreement without Giving In*, 2nd ed. (New York: Penguin, 1991).

not produce the desired outcome. Also, each party should estimate the BATNA for the other party. BATNA is the standard; it can protect both parties from accepting terms that are too unfavorable and from rejecting terms that are too favorable. A realistic BATNA is good insurance against the three decision-making traps: framing error, escalation of commitment, and overconfidence. Each party also should identify the bargaining zone, which is the gap between the two parties' BATNAs. This gap is the area of overlapping interests where agreement is possible.

(b) Conflict Management

(i) What Is Conflict Management?

Social scientists say that conflict is inevitable between people, and without conflict there is no major personal change or social progress. Conflict management involves accepting or even encouraging constructive conflict as necessary. The key point is to minimize the destructive form of conflict.

To be human is to experience conflict. This conflict arises due to differences in personal values, opinions, desires, habits, and needs of people. It is impossible for people to rise completely above selfishness, betrayals, misrepresentations, anger, and strain. The best way to depict conflict is on a scale of disruptive and destructive dimensions (see Exhibit 5.62).

EXHIBIT 5.62 Scale of Disruptive and Destructive Dimensions

Conflict at best is disruptive and at worst it is destructive. Once it erupts, conflict is difficult to control. Destructive conflict has a tendency to expand until it consumes all the things and people it touches.

When two or more people are together for any length of time, some conflict will be generated. That is inevitable. Social scientists make an important distinction between two types of conflict: realistic conflict and nonrealistic conflict (see Exhibit 5.63).

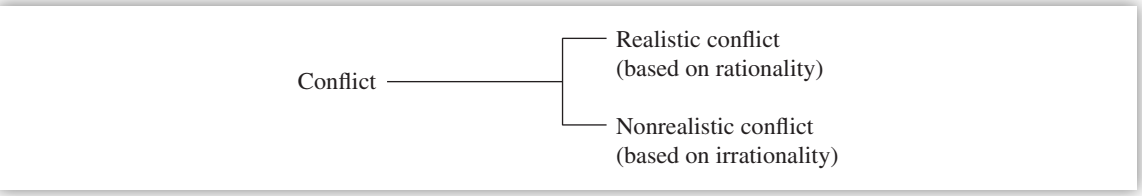


EXHIBIT 5.63 Types of Conflict

In realistic conflict, there are opposed needs, goals, means, values, or interests. Nonrealistic conflict arises from ignorance, error, tradition, prejudice, dysfunctional organizational structure, win/lose types of competition, hostility, or the need for tension release. Realistic conflict can be resolved by focusing on the emotions first followed by substantive issues and using collaborative problem-solving methods. Unrealistic conflict creates unwarranted tension between people and

can cause unnecessary destruction. Unrealistic conflict should be handled very carefully; it can be prevented to some extent.

(ii) Benefits of Conflict

Despite its drawbacks, conflict has benefits. It can spur technological development, encourage personal and intellectual growth, and help renew business organizations. Professor Richard Walton of Harvard University's Graduate School of Business noted the positive impact that conflict can have on business and other organizations. According to Walton:

> A moderate level of interpersonal conflict may have the following constructive consequences. First, it may increase the motivation and energy available to do tasks required by the social system. Second, conflict may increase the innovativeness of individuals and the system because of the greater diversity of the viewpoints and a heightened sense of necessity. Third, each person may develop increased understanding of his own position, because the conflict forces him to articulate his views and to bring forth all supporting arguments. Fourth, each party may achieve greater awareness of his own identity. Fifth, interpersonal conflict may be a means for managing the participants' own internal conflicts.

(iii) Personal Conflict Prevention and Control Methods

Although it is impossible to totally eradicate conflict, personal conflict prevention and control can avert much needless strife (unrealistic conflict). Both individuals and institutions need to develop prevention and control methods. Robert Bolton recommends:[26]

- **Use fewer roadblocks** to diminish the amount of conflict. Ordering (dominating), threatening, judging, name-calling, and other roadblocks are conflict-promoting interactions.
- **Use reflective listening** to another person when he or she has a strong need or a problem helps the other person dissipate negative emotions.

WAYS TO INCREASE ONE'S TOLERANCE AND ACCEPTANCE OF OTHERS

- Greater assertiveness
- Increased emotional support in our lives
- Effective courses in communication skills

- **Assertion skills** enable a person to get needs met with minimal strife. By asserting when needs arise, we can prevent the buildup of emotions that so often cause conflict. Both assertion and listening skills help to clear up two major sources of conflict: errors and lack of information.
- **Awareness** of which behaviors are likely to start a needless conflict between people can eliminate many confrontations. Certain words, looks, or actions tend to trigger specific people into conflict. These behaviors may be rooted in early childhood experiences. Some people can sense that a storm is brewing.

[26] Robert Bolton, *People Skills* (New York: Simon & Schuster, 1979).

HOW TO HANDLE DIFFERING POINT OF VIEWS

When another person expresses a differing point of view on a tense topic, many of us have a strong tendency to disagree argumentatively, put the other person down, or angrily denounce the person. This behavior is difficult to control, but it must be done, especially when the other person is underassertive.

- **Dumping one's bucket of tension without filling the other's bucket** is another important conflict prevention and control method. Strenuous exercise, competitive athletics, and sexual activities also can drain off one's tensions without adding to other people's stress.
- **Increased emotional support** from family and friends can decrease a person's proneness to unnecessary conflict. In general, the more we are loved and cared for, the less we need to fight.
- **Heightened tolerance and acceptance of others** also tends to diminish unrealistic conflict. Some say that these tolerances and acceptances are conditioned by upbringing and even by genetic factors. But each of us can become more tolerant and accepting than we now are.
- **Issues control** is another important way of managing conflicts. Often it is preferable to deal with one issue at a time, to break issues down into smaller units rather than deal with enormous problems with many parts, to start with easily resolved issues (i.e., start with points of agreement), and to define the dispute in nonideological terms. Try to find how your needs and the other's needs can be satisfied (i.e., win/win situation) through jointly identifying the cause of disagreement.
- **A careful appraisal of the full consequences and the cost of a conflict** may deter you from involving yourself in needless disputes. It is difficult to estimate the cost of a conflict, because emotional interactions are unpredictable and frequently get out of hand.

(iv) Group or Organizational Conflict Prevention and Control Methods

Individual actions alone are not enough. Group and/or organizational actions are needed to prevent and control the conflict that occurs in the workplace. The way an organization is structured has a bearing on the amount of conflict generated in it. The potential for conflict tends to be greater in centralized, bureaucratic organizations than in decentralized organizations. The more rigid institutions, according to Rensis Likert, have less effective communication and are less adept at managing conflict constructively than are the organizations at the other end of the continuum.

According to Bolton:[27]

- The personality and methods of the **leader** are important. Managers who have low levels of defensiveness and who are supportive tend to help people in their organizations avert unnecessary strife. A person who is in a position of power, one who has great charisma, or one who has developed effective communication skills tends to have the greatest influence on the way conflict is handled.
- The **climate** of a group also influences the amount of conflict it generates. Although some kinds of competition can be healthy, research evidence suggests that win-lose competition fosters needless conflict and diminishes the ability to resolve disputes effectively. However,

[27] Ibid.

cooperating to achieve goals that could not be accomplished without joint effort promotes more genuine harmony.

- Well-conceived and clearly stated **policies and procedures** that have the understanding and support of the relevant individuals create orderly processes that can help mitigate unnecessary chaos and conflict. When policies and procedures do not match the needs of the organization or its members, when they are arrived at arbitrarily and administered high-handedly, they can add to the level of unrealistic conflict in the organization.
- The **degree of change and the method by which change is introduced** into a family or an organization influences the amount and severity of disputes in that institution. A certain amount of change is necessary in all institutions, but too rapid a change or changes utilizing inadequate methods of communications can create significant and needless conflict.
- **Mechanisms to settle grievances** need to be established. A mechanism is practiced when resolving disputes between labor and management of an organization.
- **Training for conflict management** is necessary both for the prevention of needless conflict and for the resolution of the conflicts that are inevitable in any relationship or organization.

WHAT IS THE BEST WAY TO HANDLE CONFLICT?

Conflict management skills should be taught as part of a training program that includes listening, assertion, and collaborative problem-solving skills.

Agreed-on ways of preventing and resolving conflict, adequate channels of communication, and mechanisms for handling grievances, when combined with proper training in the areas already described, provide a comprehensive program of conflict management.

Conflict needs to be faced and resolved at the earliest possible moment. When prevention and control strategies are used improperly and unwisely, they merely postpone the inevitable. The final result is worse than an early, direct resolution of the strife.

When some people want to dodge conflict altogether, they tend to misuse the prevention and control strategies listed above. Others use denial, avoidance, capitulation, or domination as mechanisms for keeping their lives free of the unpleasantness of strife.

(c) Conflict Resolution

(i) Conflict Types

Conflict is the medium by which problems are recognized and solved. Conflict is closely related to change and interpersonal dealings. It refers to all kinds of opposition or antagonistic interaction. Not all conflict is bad. Conflict is based on scarcity of power, availability of resources, social position, and difference in value structure between individuals or groups involved in the situation. Conflict is divided into two types: functional and dysfunctional (see Exhibit 5.64).

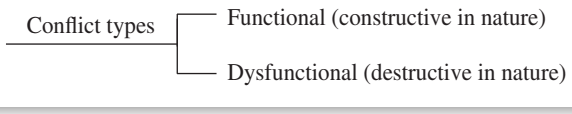


EXHIBIT 5.64 Conflict Types

- **Functional conflict.** The organizational benefits of functional conflict are increased effort and improved performance, enhanced creativity, and personal development and growth. It is like expressing anger in a constructive manner without actually showing the anger. Functional conflict is always encouraged, for obvious reasons.
- **Dysfunctional conflict.** The signs and symptoms of dysfunctional conflict include indecision, resistance to change, destructive emotional outbursts, **apathy**, and increased political maneuvering. The goal of management is to resolve or neutralize dysfunctional conflict, which is always discouraged, for obvious reasons.

(ii) Tools for Managing Conflict

Two sets of tools are available for managing conflict: conflict triggers, which stimulate conflict, and conflict resolution techniques, which are used when functional conflict deteriorates into dysfunctional conflict (see Exhibit 5.65).

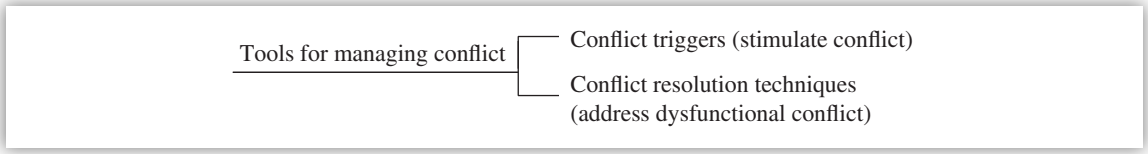


EXHIBIT 5.65 Tools for Managing Conflict

(A) Conflict Triggers A conflict trigger is a factor or circumstance that increases the choices of intergroup or interpersonal conflict. It can stimulate either functional or dysfunctional conflict, where the former should be continued and the latter should be removed or corrected. According to Kreitner,[28] examples of major conflict triggers include:

- Ambiguous or overlapping jurisdictions. (Reorganization will help to clarify job boundary problems.)
- Competition for scarce resources. (This includes funds, personnel, authority, power, and valuable information.)
- Communication breakdowns. (Communication barriers provoke conflict. Clear communications should be practiced.)
- Time pressures. (Deadlines can prompt performance or trigger destructive emotional reactions.)
- Unreasonable standards, rules, policies, or procedures. (These can lead to dysfunctional conflict between managers and their subordinates. The solution is to correct the situation.)
- Personality clashes. (A solution is to separate the antagonistic parties by reassigning one or both to a new job.)
- Status differentials. (Job hierarchy creates status differentials that lead to dysfunctional conflict. This can be minimized by showing a genuine concern for the ideas, feelings, suggestions, and value of subordinates.)
- Unrealized expectations. (Dysfunctional conflict is another by-product of unrealized expectations. This can be avoided by taking the time to discover what people expect from their employment.)

[28] Kreitner, *Management*.

(B) Conflict Resolution Techniques Managers have two choices in resolving conflict: do nothing, which is not a good strategy, or try one or more of the five conflict resolution techniques:

1. Problem solving
2. Superordinate goals
3. Compromise
4. Forcing
5. Smoothing

See Exhibit 5.66.

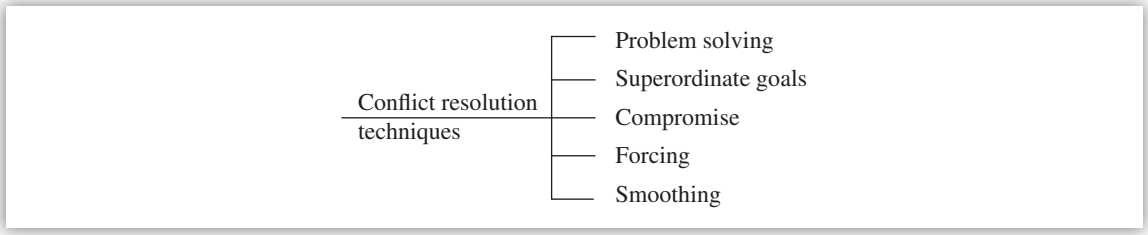


EXHIBIT 5.66 Conflict Resolution Techniques

- **Problem solving.** Problem solving encourages managers to focus their attention on root causes, factual information, and promising alternatives rather than on personalities or scapegoats. It is a time-consuming process but it is worth it.
- **Superordinate goals.** Superordinate goals are highly valued, unattainable by any one group or individual alone, and commonly sought. The manager brings the conflicting parties together and tries to resolve the dysfunctional conflict.
- **Compromise.** Everybody wins and loses because compromise requires negotiation, or give-and-take. Compromise is based on the idea that "something must be given up if anything is to be gained." It is a time-consuming process, and the problem is worked around rather than solved.
- **Forcing.** Management steps into a conflict and orders the affected parties to handle the situation in a certain manner. It is based on the formal authority and power of superior position. Forcing does not resolve the personal conflict; in fact, it could compound the situation by hurting feelings, fostering resentment, and creating mistrust.
- **Smoothing.** Smoothing is a temporary, short-term action that does not solve the underlying problem. It can be useful when management is attempting to hold things together until a critical project is completed, there is no time for problem solving or compromise, or forcing is deemed inappropriate. Smoothing is appropriate in some situations but not all.

KEY CONCEPTS TO REMEMBER: Conflict Management

Problem solving is the only long-term approach that removes the actual sources of conflict. The other four approaches amount to short-term, stopgap measures. When time is available, problem solving is the preferred approach. When time is not available, management may choose to fall back on the other four approaches: superordinate goals, compromise, forcing, or smoothing.

According to Dean Tjosvold,[a] conflicts, when appropriately measured, add substantial value to organizations. Employees who discuss conflicts disclose information, challenge assumptions, dig into issues, and, as a consequence, make successful decisions. Conflict is necessary because diverse opinions and information are mandatory for problem solving and getting things done in organizations.

[a]Dean Tjosvold, *Learning to Manage Conflict: Getting People to Work Together Productively* (New York: Lexington Press, 1993).

(iii) Another Perspective on Conflict Resolution

How do we resolve conflict? The conflict resolution method can be thought of as a set of rules and regulations that govern conflict. Without rules and regulations, conflict can get out of hand in both personal and work life. Conflict resolution techniques stress the importance of rationally examining specific issues at the outset. In conflict resolution, the first goal is to deal constructively with the emotions. A useful distinction can be made between the emotional and the substantive aspects of conflict (see Exhibit 5.67).

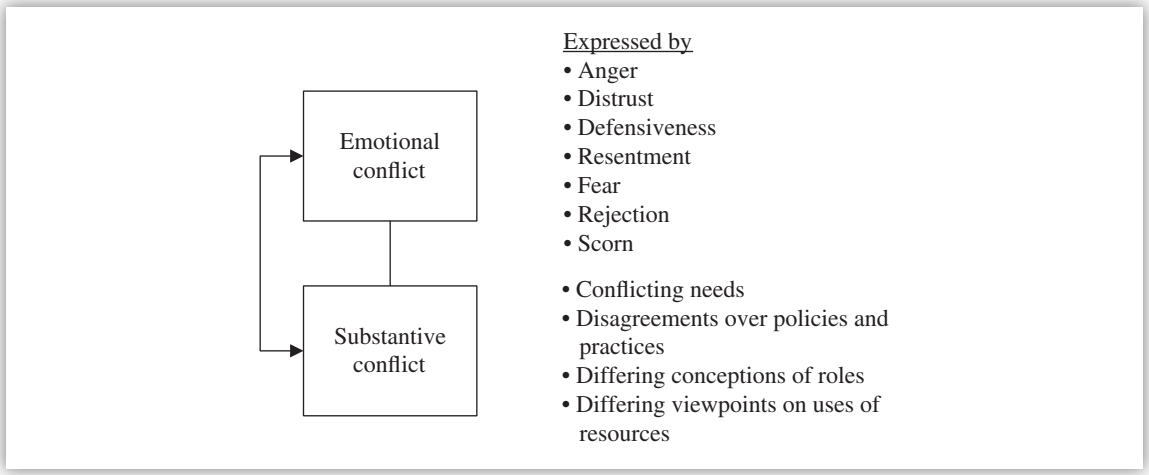


EXHIBIT 5.67 Distinction between Emotional Conflict and Substantive Conflict

When feelings are strong, it is usually a sound strategy to deal with the emotional aspects of conflict first. Substantive issues can be handled more constructively once the emotions have subsided. These two aspects of conflict interact with one another and are often intertwined and difficult to separate. Substantive conflict often generates emotional conflict. Conversely, emotional conflict may multiply the substantive issues. However, both dimensions need to be handled properly.

Bolton[29] suggests a three-step process of conflict resolution to help people argue constructively in a systematic, noninjurious, and growth-producing way.

(A) Step 1: Treat the Other Person with Respect Respect for another person is an attitude conveyed by specific behaviors. The way we listen to the other person or look at him or her, our tone of voice, our selection of words, the type of reasoning we use—these either convey respect or they communicate disrespect.

[29] Bolton, *People Skills.*

Unfortunately, a disagreement with another person's beliefs or values or a conflict of needs often degenerates into disrespect for both the other person's ideas and personhood. Even when we respect another person, in the heat of conflict, we are apt to disparage him or her.

Some people think their disrespectful thoughts but do not say them outright. However, when your attitude toward another is disrespectful, your body language whispers the truth. The other party may read it in your facial expression, tone of voice, gestures, and so on. This also blocks the conversation and may cause long-term damage to the relationship. We all tend to stereotype one another. When this happens, we talk at each other or past each other, not *with* each other.

For many of us, an act of willpower is needed to fight the gravitational pull into disrespect. The exertion of moral force is required to treat the other individual as a person of worth with whom we will enter into a dialogue as equals.

(B) Step 2: Listen until You "Experience the Other Side" Under the best conditions, effective communication is difficult to achieve. During conflict, when feelings are strong, people are especially prone to misunderstanding one another. It is very difficult to accurately understand and summarize another person's point of view during disagreements. *People often hear from their own point of view and reflect back a summary that is correct in many ways but that distorts the other's message.*

The best thing to do is to concentrate on reflecting feelings. It is not enough to hear the other's emotions—they need to be understood and accepted. Sometimes the actions of the other person will seem like a deliberate attempt to hurt you. You will be tempted to strike back in rage. If you choose to resist that impulse and empathetically reflect the other party's feelings, you will be amazed at how quickly the other's feelings usually subside. "Keep cool" is sound advice.

KEY CONCEPTS TO REMEMBER: Dos and Don'ts of Conflict Management

Don't say "I know how you feel." The other person will rarely believe it because you really don't know how that person feels.

Don't offer explanations, apologies, or make any other statements at this point.

Do discipline yourself to understand the opinions and suggestions or feelings of the other person—from his or her point of view—and then reflect those thoughts and feelings back to the other in succinct statements.

Do maintain silence to let the other negotiator think about what you have said, indicate that it was essentially correct, and explain his or her point a bit further or correct any inaccuracies there may have been in the other's speaking or your listening. If the other person adds to what he or she said or corrects your reflection, summarize that to the other's satisfaction. When the other person feels heard, you have earned the right to speak your point of view and express your feelings.

(C) Step 3: State Your Views, Needs, and Feelings After demonstrating respect for the other party as a person and conveying your understanding of his or her feelings and point of view, it is your turn to communicate your meaning. Five guidelines are useful at this step of the conflict resolution process.

1. State your point of view briefly. Keep the message short and to the point.
2. Avoid loaded words. Conversation is not just crossfire where you shoot and get shot at!

3. Say what you mean and mean what you say. Don't withhold important information in tense times. State the truth.
4. Disclose your feelings. It is difficult to constructively express the alienation you feel toward the person who has offended you, but normally this needs to be done if the conflict is to be resolved.
5. Be flexible. Sometimes one person is upset and the other is not. When the angry person vents feelings and is accepted and treated with respect, the conflict may end.

(iv) Ways to Implement the Conflict Resolution Method

According to Bolton,[30] there are four ways of implementing the conflict resolution method (see Exhibit 5.68). First, you can use this method even when the other person is not using it. By listening to the other person with respect and speaking briefly in noninflammatory ways, you can help the other person to simmer down and engage in a more productive discussion.

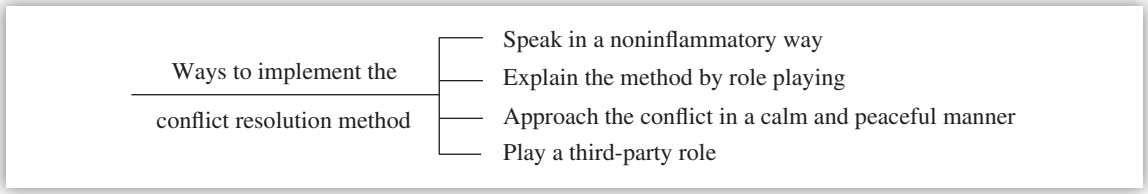


EXHIBIT 5.68 Ways to Implement the Conflict Resolution Method

When you are involved in a dispute or sense that a fight is brewing, a second approach is to explain the method briefly and ask the other person to join you in trying this way of relating. Perhaps you might explain the method by role-playing it. Treat the other person with respect, listen carefully to the objection, and demonstrate that you understand.

A third way of introducing the conflict resolution method is to do so beforehand, when things are calm and peaceful. This means explaining that conflict is inevitable in any group and there is a way of successfully coping with the emotional elements of conflict so that people can discuss their differences more profitably and resolve them more constructively.

Finally, you can use this method to help others resolve their conflicts by playing a third-party role. It is important to remain neutral and make sure that the conflict resolution process is followed properly. The third party can summarize the major issues raised by each person. The role of the third party is to stay out of the conflict, help others use a method by which they can communicate under stress, and help them learn a method that will enable them to handle further conflicts successfully without third-party assistance.

IT IS OK TO DISAGREE!

- When this conflict resolution method is used to abate values clashes, the goal is to understand one another better, perhaps influence each other to some degree, and to agree to disagree on the issues that remain.
- This process enables the parties to communicate face to face until acceptance of the right to differ occurs. People can remain at odds in terms of some issues without being at odds with each other.

[30] Bolton, *People Skills.*

(v) Collaborative Problem Solving

(A) Types of Conflict According to Bolton,[31] three kinds of conflict exist: conflict of emotions, value conflicts, and conflict of needs (see Exhibit 5.69).

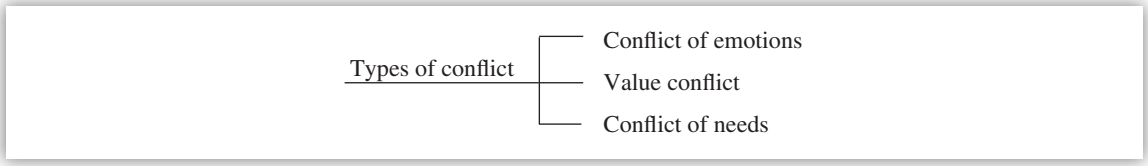


EXHIBIT 5.69 Types of Conflict

Conflict of emotions is inevitable because of differences in people. It can be resolved using the conflict resolution method outlined earlier. There is rarely any "solution" to a **value conflict** situation because nothing concrete or tangible is involved for the person who is upset. In this situation, the use of the conflict resolution method may help people with opposing beliefs to better understand one another, help them to develop more tolerance for each other's position, and occasionally influence their attitudes and actions. A collaborative problem-solving method is usually used to handle a **conflict of needs** situation.

(B) An Elegant Solution In collaborative problem solving, once people discover they have conflicting needs, they join together to find a solution acceptable to both. Doing so entails redefining the problem, discovering alternatives, and focusing on overlapping interests. In this process, neither person capitulates to or dominates the other. Because no one loses, no one gives up or gives in, and because all parties benefit, this is often called a win-win way of dealing with conflicting needs. Collaborative problem solving is usually the most desirable way to resolve the conflicts of needs that occur between people. It is different from other ways of dealing with conflicting needs, such as win-lose, lose-lose, mini-lose–mini-lose.

WIN-WIN OUTCOME VERSUS WIN-LOSE OUTCOME

- Win-win outcome requires a needs-based definition of a problem.
- Win-lose outcome results from focusing on a solution-type definition of a problem.

To realize a win-win outcome, you need to state interpersonal problems in terms of needs rather than solutions. This requires making statements in terms of what, why, and how. The reason is that solution-type definitions lead to win-lose results. Redefinition of the problem in terms of specific needs leads to conflict resolution in which all parties can get their needs met. One important thing in this process is to distinguish between means and ends. As the old saying goes, "A problem well defined is half solved." The adage is easy to say but, in reality, it is difficult to assert one's own needs, listen reflectively, and then restate both sets of needs in a summary manner.

While there is no guarantee that the following steps will work all the time, they will prove useful a great majority of the time. There are six steps to the collaborative problem-solving method.

1. Define the problem in terms of needs, not solutions.
2. Brainstorm possible solutions.

[31] Ibid.

3. Select the solution(s) that will best meet both parties' needs and check possible consequences.
4. Plan the implementation.
5. Implement the plan.
6. Evaluate the process.

These six steps are similar in any problem-solving situation.

COMMON BARRIERS TO THE COLLABORATIVE PROBLEM-SOLVING PROCESS

- Not handling the emotions first
- Not dealing with the problem properly
- Evaluating or clarifying during brainstorming
- Not working out the details
- Not following up to see that the action steps are carried out

(C) Alternatives to Collaborative Problem Solving There are four fairly common alternatives to collaborative problem solving: (1) denial, (2) avoidance, (3) capitulation, (4) and domination (see Exhibit 5.70). Excessive, repeated use of any of these options leads to predictable negative consequences.

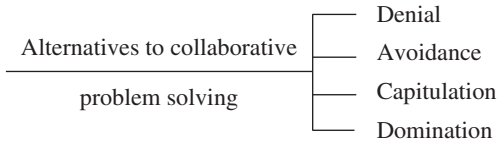


EXHIBIT 5.70 Alternatives to Collaborative Problem Solving

Denial Conflicts are so threatening to some people that they simply deny the existence of interpersonal problems. They do nothing about the problem except exclude it from conscious awareness. Repeated denial can lead to psychosomatic illness and other forms of psychological distress.

Avoidance Some people are aware of interpersonal conflicts of needs; they simply do everything within their power to avoid facing them. They withdraw from situations when strife occurs, or they gloss over the problem, acting as though it does not exist. Repeated avoidance of problems can result in a greatly diminished existence, and continued avoidance leads to denial.

Capitulation Capitulation occurs when people surrender or give in when someone else's needs conflict with their own needs; they feel that their needs will not be met, so it is useless to try. Repeated use of denial, avoidance, and capitulation approaches, either alone or in combination, amount to submissive behavior. The negative consequences of submissive behavior are listed next.

- Submissive people do not call their own plays. Others choose the course of action for submissive people.
- Their relationships tend to be less satisfying.
- They cannot control their own negative emotions. Pent-up emotions cause more damage. Certain diseases are caused by or aggravated by submissive behavior (e.g., headaches, ulcers, skin diseases, arthritis).

Domination Domination (competing) is imposing one's own solution on the other person. The person who dominates decision making comes up with a solution to meet his or her own needs. *Aggressive people tend to rely on domination during a conflict of needs.*

When domination occurs repeatedly, the negative results are often dramatic. People resort to sabotage, pilferage, work stoppage, passive resistance, emotional distance, and other destructive ways of striking back.

(D) What Is the Solution? *Accommodation and compromise* are good solutions for solving interpersonal differences. Accommodation is the intention of one party to sacrifice for others. One party places the opponent's interests above his or her own in the interest of maintaining good relations. Supporting others' opinions and forgiving others for an infraction are examples of accommodation.

Compromise is consent reached by mutual concessions. It takes into account the needs and fears of both parties. In a world of conflicting needs, wants, and values, compromise does have its place. However, when used exclusively, it can lead to very undesirable results. This is because with compromise, each party settles for something less than its full needs and desires (the mini-lose–mini-lose method). Each side gives something up to end the conflict or solve the problem. Again, although this is perfectly acceptable in some negotiations, it is not ideal for all situations.

(d) Added-Value negotiating

(i) Description

Added-value negotiating (AVN) is a value-added process (win-win) involving development of multiple deals with multiple outcomes as opposed to traditional (win-lose) negotiating, which is based on a single outcome with a single winner.

According to Kreitner,[32] AVN is based on openness, flexibility, and a mutual search for the successful exchange of value. AVN allows one to build strong relationships with people over time. It bridges the gap between win-win theory and practice.

(ii) Specific Steps

According to Kreitner,[33] AVN comprises the following five steps:

1. **Clarify interests.** Both parties jointly identify subjective and objective interests so that a common goal is found.

[32] Kreitner, *Management*, originally from Carl Albrecht and Steve Albrecht, "Added-Value Negotiating," *Training Magazine* (April 1993).
[33] Kreitner, *Management*.

2. **Identify options.** A variety of choices are developed to create value for both parties.
3. **Design alternative deals.** Multiple win-win offers are designed to promote creative agreement.
4. **Select a deal.** Each party selects a mutually acceptable deal after testing the various deals for value, balance, and fit.
5. **Perfect the deal.** Unresolved details are openly discussed, and agreements are put in writing.

5.5 Project Management and Change Management

Two major topics such project management techniques (e.g., PERT and CPM) and change management methods are described in this section.

(a) Project Management Techniques

In order for projects to be successfully implemented, they must be well managed. Many organizations apply a variety of project management techniques to optimize project success and enhance the likelihood of meeting project-specific as well as organization-wide goals. These techniques include monitoring project performance, establishing incentives to meet project goals, and developing a project management team with the right people and the right skills. This can help avert cost overruns, schedule delays, and performance problems common to many organizations.

It is important to develop **performance measures** and link project outcomes to business unit and strategic goals and objectives. The key is monitoring project performance and establishing incentives for accountability, and using cross-functional teams to involve those with the technical and operational expertise necessary to plan and manage the project.

Typically, a **project plan** is used to manage and control project implementation. It includes performance measurement baselines for schedule and cost, major milestones, and target dates and risks associated with the project. By tracking cost, schedule, and technical performance, a project team is aware of potential problem areas and is able to determine any impact of the deviation and decide if corrective action is needed. Regular review of the status of cost, schedule, and technical performance goals by individuals outside the project team allows for an independent assessment of the project and verification that the project is meeting stated goals.

Major projects should include **multidisciplinary teams**, consisting of individuals from different functional areas and led by a project manager, to plan and manage projects. Typically, a core project team is established early in the life cycle of a project, and additional individuals with particular technical or operational expertise are added during appropriate phases of the project. The team must not only possess technical and operational expertise, but it must also be composed of the "right" people. The selection of the team members is critical—they must be knowledgeable, willing to trade off leadership roles, and able to plan work and set goals in a team setting. The successful team will have a high spirit, trust, and enthusiasm. A sense of ownership and the drive of the team committed to a project are key factors in the successful completion of a project. This integrated and comprehensive approach improves communication between upper management and project managers and among the various stakeholders in the project. It also increases the likelihood that potential problems will be identified and resolved quickly, thus increasing the chances that the project will remain on schedule and within budget.

(i) Why Project Management?

Management needs to know what parts of the project or program are most likely to cause serious delays. This knowledge will lead to management actions that will achieve the project or program objectives and deadlines.

When is project management preferred? The project management approach is the preferred method for dealing with projects defined once. The task is very complex and involves interdependence between a number of departments. The task has great significance to the organization. Onetime tasks can be accomplished with a minimum interruption of routine business.

Managers need to coordinate diverse activities toward a common goal. Management must devise plans that will tell with reasonable accuracy how the efforts of the people representing these functions should be directed toward the project's completion. In order to devise such plans and implement them, management must be able to collect pertinent information to accomplish the following tasks:

- To form a basis for prediction and planning
- To evaluate alternative plans for accomplishing the objective
- To check progress against current plans and objectives
- To form a basis for obtaining the facts so that decisions can be made and the job can be done

A single master plan for a project should include planning, scheduling, and controlling functions. The plan should point directly to the difficult and significant activities—the problem of achieving the objective. For example, the plan should form the basis of a system for management by exception. It should indicate the exceptions (red flags). Under such a system, management need act only when deviations from the plan occur.

A reporting system should be designed for middle to senior management to use. The monthly progress report calls for specific reestimate only for those events on critical paths and subcritical events. The report should accomplish these tasks:

- Preparing a master schedule for a project
- Revising schedules to meet changing conditions in the most economical way
- Keeping senior management and the operating department management advised of project progress and changes

Plans should be separated from scheduling. Planning is the act of stating what activities must occur in a project and in what order these activities must take place. Scheduling follows planning and is defined as the act of producing project timetables in consideration of the plan and costs. Controlling is ensuring that plans are accomplished. The correct sequence is

$$\text{Planning} \rightarrow \text{Scheduling} \rightarrow \text{Controlling}$$

Project structure is a characteristic of all projects that provides for all work being performed in some well-defined order. For example: In R&D and product planning, specifications must be

determined before drawings can be made. In advertising, artwork must be made before layouts can be done. Exhibit 5.71 shows factors responsible for a successful performance of a project as well as symptoms of project management failures.

Factors responsible for successful performance of a project	Symptoms of project management failures
Organization of the project	High costs
Authority of the project manager	Schedule overruns
Scheduling and planning techniques used	Poor-quality product
The project manager's good relationship with senior management	Failure to meet project objectives
Use of resources, including slack time	Customer or user dissatisfaction with the end result

EXHIBIT 5.71 Successful Factors and Symptoms of Project Management Failures

(ii) Project Management's Basic Guidelines

The following list provides basic guidelines for project management.

1. **Define the objective(s) of the project.** This includes defining management's intent in undertaking the project, outlining the scope of the project, and describing the end results of the project including its effects on the organization.
2. **Establish a project organization.** This includes appointment of one experienced manager to run the project full time, organization of the project management function in terms of responsibilities, assignment of manpower to the project team, and maintenance of a balance of power between the functional department managers and the project manager.
3. **Install project controls.** This includes controls over time, cost, and quality.

(iii) Project Organization

Project organization is where the reporting relationships and the work location rest predominantly with the project manager. Three common types of project organization include traditional structure, matrix organization, and hybrid form (see Exhibit 5.72).

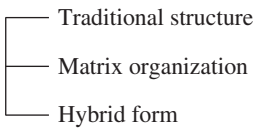


EXHIBIT 5.72 Types of Project Organization

In a **traditional structure**, the basic interrelationship is with the functional manager. A hierarchy of reporting relationships is followed. In a **matrix organization**, most of the personnel are directly responsible to the project manager for work assignments but remain physically located with their functional manager. Other forms of organization include combining a large project team with several small functional teams or basic functional teams with a small project task force.

Matrix team members must learn new ways of relating and working together to solve cross-functional problems and to attain synergy. According to Dr. Jack Baugh,[34] the matrix management structure must be used when there is:

1. A rapid technological advancement, a need for timely decisions.
2. A vast quantity of data to be analyzed.
3. An increased volume of new products and services to be introduced.
4. A need for simultaneous dual decision making.
5. A strong constraint on financial and/or HRs.

Baugh also cited reasons for using a matrix management structure. According to Baugh, such a structure:

1. Provides a flexible adaptive system.
2. Provides timely, balanced decision making.
3. Permits rapid management response to a changing market and technology.
4. Trains managers for ambiguity, complexity, and executive positions.
5. Helps in synergizing and motivating human resources.

The **hybrid form** is the best possible option since it can achieve technical excellence and, at the same time, meet cost and schedule deadlines.

Project authority is a measure of the degree of control the project manager has over all the activities necessary to complete the project successfully. Delays can be reduced if the project manager can make decisions without having to wait for the approval of someone higher up. This type of delay is often the cause of schedule and cost overruns.

The authority of the project manager is seldom spelled out in formal directives or policies. The traditional forms of management—one person, one boss—is simply not adequate for completing projects.

The conflict is between the project manager and the functional manager. It is the influence rather than authority that matters. What counts is the priority assigned to the project and the experience and personal characteristics of the project manager. *There may not be any relation between the formal authority of the project manager and the actual success of the project.*

KEY CONCEPTS TO REMEMBER: Most Common Reasons for Project Management Failures

- The basis for a project is not sound.
- The wrong person is appointed as the project manager.

[34] *WINGS: Project Leaders Guide,* Vols. 1 and 2 (King of Prussia, PA: AGS Management Systems, 1986). Original citation by Dr. Jack Baugh of Hughes Aircraft Company.

- Company management fails to provide enough support.
- Task definitions are inadequate.
- Management monitoring techniques are not appropriate.
- Project termination is not planned properly (i.e., to reduce adverse effect on the employee's progress in the company after the project is completed).
- Redefinitions of the project's scope are unclear.
- Large-scale design changes are occurring.
- Additional funding is not approved.

(iv) Problems in Project Management

Project managers face unusual problems in trying to direct and harmonize the diverse forces at work in the project situation. Their main difficulties arise from three sources: organizational uncertainties, unusual decision pressure, and inadequate senior management support (see Exhibit 5.73).

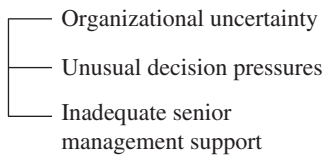


EXHIBIT 5.73 Nature of Project Problems

(A) Organizational Uncertainty In a situation of organizational uncertainty, the working relationships between the project manager and the functional department managers have not been clearly defined by senior management. Uncertainties arise with respect to handling delays, cost overruns, work assignments, and design changes. Unless the project manager is skillful in handling these situations, senior management may resolve them in the interest of functional departments, at the expense of the project as a whole.

(B) Unusual Decision Pressures When uncertainties are added to the situation, the project manager has to make decisions based on limited data and with little or no analysis. The project manager must move fast, even if it means an intuitive decision that might expose him or her to senior management criticism. *Decisions to sacrifice time for cost, cost for quality, or quality for time are common in most projects.* There is a clear indication that the project manager needs support from senior management due to these trade-offs.

(C) Inadequate Senior Management Support Senior management seldom can give the project manager as much guidance and support as his or line counterpart gets. Delays in initial approval of the project by senior management, inability to resolve conflicts between the project manager and the functional department managers, and delays in allocating resources are the most common issues on which the project manager needs more attention from senior management. Otherwise, project performance can be hampered.

(v) Project-Scheduling Techniques The six project-scheduling techniques discussed in this section are listed next.

1. Program evaluation and review techniques
2. Critical path methods
3. Line-of-balance method
4. Graphical evaluation and review techniques
5. Work breakdown structure
6. Gantt chart

(See Exhibit 5.74.)

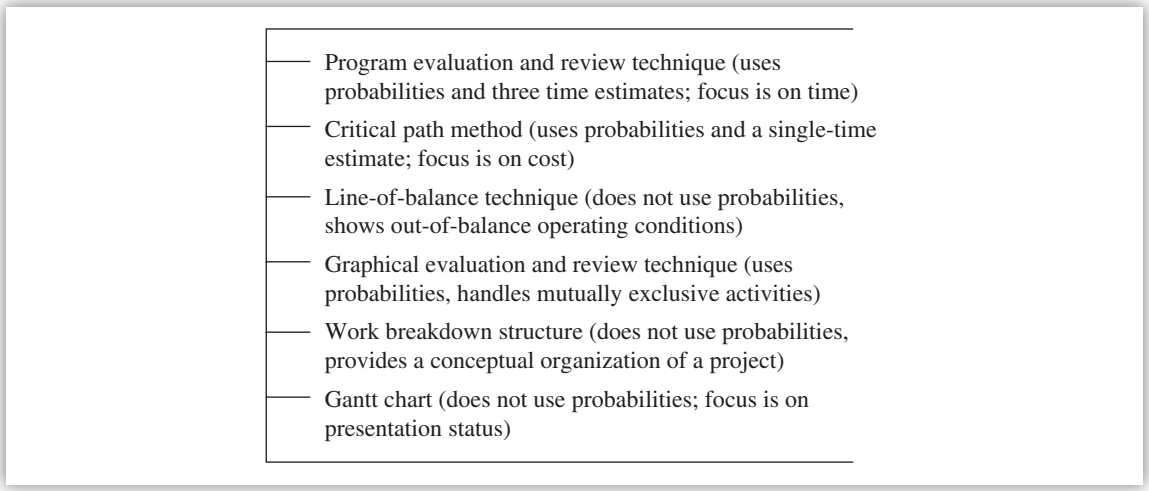


EXHIBIT 5.74 Project-Scheduling Techniques

(A) Program Evaluation and Review Techniques Project management frequently uses network diagrams to plan the project, evaluate alternatives, and control large and complex projects toward completion. PERT requires extremely careful plans from the very outset of the project. These careful plans allow management to allocate resources to critical areas before they become critical. Doing so will alert a manager to trouble areas or bottlenecks before they become a major problem and the source of a project overrun. PERT also helps to allocate resources but has no influence on the excellence of the end product.

PERT improves communication upward to the manager and the customer (client). PERT lets the supervisor believe that the project manager is doing a superior job, regardless of how well the project manager is actually performing.

PERT Features Features of PERT are listed next.

- PERT manages one-of-a-kind programs as opposed to repetitive tasks. It develops a network diagram that identifies the sequence of events and their relationships to one another along with estimated start and completion times.

SENSITIVITY ANALYSIS AND PERT

Sensitivity analysis can be performed on the PERT network. This analysis provides the ability to check the feasibility of current schedules and to permit management to experiment with or evaluate the effects of proposed changes.

- Uncertainties involved in programs can be handled where no standard cost and time data are available.
- PERT includes a network comprised of events and activities. An event represents a specified program accomplishment at a particular instant in time. An activity represents the time and resources, which are necessary to progress from one event to the next.
- Events and activities must be sequenced on the network under a highly logical set of two ground rules, which allow the determination of critical and subcritical paths. The ground rules are: (1) No successor event can be considered completed until all of its predecessor events have been completed; and (2) no looping is allowed (i.e., no successor event can have an activity dependency that leads back to a predecessor event).
- Time estimates are made for each activity of the network on a three-way basis: optimistic, most likely, and pessimistic. The three time estimates are required as a gauge of the "measure of uncertainty" of the activity and represent the probabilistic nature of many tasks. The three estimates are reduced to a single expected time and a statistical variance.

PERT Assumptions Interrelationships of activities are depicted in a network of directed arcs (arcs with arrows, which denote the sequence of the activities they represent). The **nodes**, called events, represent instants in time when certain activities have been completed and others can then be started. All inward-directed activities at a node must be completed before any outward-directed activity of that node can be started. A **path** is defined as an unbroken chain of activities from the origin node to some other node. The origin node is the beginning of the project. An **event** is said to have occurred when all activities on all paths directed into the node representing that event have been completed.

Another assumption of PERT is that all activities are started as soon as possible. This assumption may not hold true when scarce resources must be allocated to individual activities.

PERT Applications The development of a critical path network is accomplished by establishing the major milestones that must be reached. Construction of the network diagram requires identification and recording of the project's internal time dependencies—dependencies that might otherwise go unnoticed until a deadline slips by or impacts other activities. A new activity can be added by identifying its successor and predecessor.

An ordered sequence of events to be achieved would constitute a valid model of the program. The network provides a detailed, systematized plan and time schedule before the project begins. As the project progresses, the time estimates can be refined. A top-down approach is taken when developing the network. The total project is fully planned, and all components of the plan are included.

APPLICATIONS OF PERT AND CPM

- Construction and maintenance of chemical plant facilities, highways, dams, buildings, railroads, and irrigation systems
- Planning of retooling programs for high-volume products in plants such as automotive and appliance plants
- Introduction of a new product
- Installation of a computer system
- Acquisition of a company

Critical path scheduling helps coordinate the timing of activities on paper and helps avert costly emergencies. The network diagram must be developed in detail as much as possible so that discrepancies, omissions, and work coordination problems can be resolved inexpensively, at least to the extent that they can be foreseen.

Project diagrams of large projects can be constructed by sections. Within each section, the task is accomplished one arrow at a time by asking and answering the following questions for each job:

- What immediately preceded this job?
- What immediately succeeds (follows) this job?
- What can be concurrent with this job?

If the maximum time available for a job equals its duration, the job is called critical. A delay in a critical job will cause a comparable delay in the project completion time. A project contains at least one contiguous path of critical jobs through the project diagram from beginning to end. Such a path is called a critical path.

MEANING OF THE CRITICAL PATH

Typically only about 10% to 15% of the jobs in a large project are critical. The primary purpose of determining the critical path is to identify those activities that must be finished as scheduled if the new program or project is to be completed on time. The critical path of those activities cannot be delayed without jeopardizing the entire program or project.

If the maximum time available for a job exceeds its duration, the job is called a **floater**. Some floaters can be displaced in time or delayed to a certain extent without interfering with other jobs or the completion of the project. Others, if displaced, will start a chain reaction of displacements downstream in the project.

The technological ordering is impossible if a cycle error exists in the job data (i.e., job a preceded b, b precedes c, and c precedes a). The time required to traverse each arrow path is the sum of the times associated with all jobs on the path. The critical path (or paths) is the longest path in time from start to finish; it indicates the minimum time necessary to complete the entire project.

In order to accurately portray all predecessor relationships, dummy jobs often must be added to the project graph. The critical path is the bottleneck route; only by finding ways to shorten jobs along the critical path can the overall project time be reduced; the time required to perform noncritical jobs is irrelevant from the viewpoint of total project time.

PERT Approach The status of a project at any time is a function of several variables, such as resources, performance, and time. Resources are in the form of dollars or what "dollars" represent—manpower, materials, energy, and methods of production; and technical performance of systems, subsystems, and components. An optimum schedule is the one that would properly balance resources, performance, and time.

Information concerning the inherent difficulties and variability in the activity being estimated are reflected in the three numbers: The optimistic, pessimistic, and most likely elapsed time estimates should be obtained for each activity. The purpose of the analysis is to estimate, for each network event, the expected times (mean or average) and expected calendar time of occurrence.

When PERT is used on a project, the three time estimates (optimistic, most likely, and pessimistic) are combined to determine the expected duration and the variance for each activity.

- **Optimistic.** An estimate of the minimum time an activity will take. This is based on everything going right the first time. It can be obtained under unusual, good-luck situations.
- **Most likely.** An estimate of the normal time an activity will take, a result that would occur most often if the activity could be repeated a number of times under similar circumstances.
- **Pessimistic.** An estimate of the maximum time an activity will take, a result that can occur only if unusually bad luck is experienced.

The expected times determine the critical path and the variances for the activities on this path are summed to obtain the duration variance for the project. A probability distribution for the project completion time can be constructed from this information. However, the variances of activities that do not lie on the critical path are not considered when developing the project variance, and this fact can lead to serious errors in the estimate of project duration.

An estimate of the length of an activity is an uncertain one. A stochastic model can be used to reflect this uncertainty. This model measures the possible variation in activity duration. It may take the form of a distribution showing the various probabilities that an activity will be completed in its various possible completion times. Alternatively, it may be nondistribution, such as range or standard deviation.

$$\text{Expected time} = 1/6\ (a + 4m + b)$$

where a = Optimistic time
m = Most likely time
b = Pessimistic time

The expected activity times derived from a three-estimate, PERT-type calculation provides a more accurate estimate and allows the activity time variance to be calculated and included in the estimates of project duration.

APPLICATION OF PERT

Example

A company is planning a multiphase construction project. The time estimates for a particular phase of the project are

Optimistic	2 months
Most likely	4 months
Pessimistic	9 months

Question: Using PERT, what is the expected completion time for this particular phase?

Answer: The expected completion time would be 4.5 months, as shown next.

$$\text{Expected time} = 1/6\,(a + 4m + b) = 1/6\,(2 + 4 \times 4 + 9) = 27/6 = 4.5.$$

The latest calendar time at which an event must be accomplished so as not to cause a slippage in meeting a calendar time for accomplishing the objective event is referred to as the latest time (denoted TL). The difference between the latest and expected times, TL – TE, is defined as **slack**. Slack can be taken as a measure of scheduling flexibility that is present in a workflow plan, and the slack for an event also represents the time interval in which it might reasonably be scheduled. Slack exists in a system as a consequence of multiple path junctures that arise when two or more activities contribute to a third.

WHAT IS SLACK TIME?

Slack time is a free time associated with each activity as it represents unused resources that can be diverted to the critical path. Noncritical paths have slack time while critical paths have no slack time.

A slack is extra time available for all events and activities not on the critical path. A negative slack condition can prevail when a calculated end date does not achieve a program date objective established earlier.

The manager must determine valid means of shortening lead times along the critical path by applying new resources or additional funds, which are obtained from those activities that can afford it because of their slack condition. "Safety factor" is another name for "slack." Alternatively, the manager can reevaluate the sequencing of activities along the critical path. If necessary, those activities that were formerly connected in a series can be organized on a parallel or concurrent basis, with the associated trade-off risks involved. Alternatively, the manager may choose to change the scope of work of a critical path alternative in order to achieve a given schedule objective.

When some events have **zero slack**, it is an indication that the expected and latest times for these events are identical. If the zero-slack events are joined together, they will form a path that will extend from the present to the final event. This path can be looked on as the critical path. Should any event on the critical path slip beyond its expected date of accomplishment, then the final event can be expected to slip a similar amount. The paths having the greatest slack can be examined for possible performance or resource trade-offs.

When jobs or operations follow one after another, there is no slack. The criteria for defining a subcritical event is related to the amount of slack involved in the event. Those events having as much as five weeks slack are considered subcritical.

PERT analysis permits a quantitative evaluation of conceivable alternatives. Each job in the project is represented by an arrow, which depicts the existence of the job and the direction of time flows from the tail to the head of the arrow. The arrows are then connected to show graphically the sequence in which the jobs in the project must be performed. The junctions where arrows meet are called events. These are points in time when certain jobs are completed and others must begin.

The difference between a job's early start and its late start (or between early finish and late finish) is called total slack (TS). Total slack represents the maximum amount of time a job may be delayed beyond its early start without necessarily delaying the project's completion time.

KEY CONCEPTS TO REMEMBER: Pert Time Dimensions

ES = Earliest start time for a particular activity
EF = Earliest finish time for a particular activity
EF = ES + *t*, where *t* is expected activity time for the activity
LS = Latest start time for a particular activity
LF = Latest finish time for a particular activity
LS = LF – *t*, where *t* is expected activity time for the activity
Total slack time (TS) = LS – ES or LF – EF
Free slack time (FS) = EF – ES

The manager examines the work demand and indicates if sufficient resources are available to accomplish all jobs by their early finish. If resources are insufficient, activities are rescheduled within their late finish, using project priority and available slack. Later, the manager is asked for additional resources or for a decision to delay an activity beyond its late finish.

Critical jobs are those on the longest path throughout the project. That is, critical jobs directly affect the total project time.

If the target date (T) equals the early finish date for the whole project (F), then all critical jobs will have zero total slack. There will be at least one path going from start to finish that includes critical jobs only—that is, the critical path. There could be two or more critical paths in the network, but only one at a time.

If T is greater (later) than F, then the critical jobs will have total slack equal to T minus F. This is a minimum value; since the critical path includes only critical jobs, it included those with the smallest TS. All noncritical jobs will have greater total slack.

Another kind of slack is **free slack** (FS). It is the amount a job can be delayed without delaying the early start of any other job. A job with positive total slack may or may not also have free slack, but the latter never exceeds the former. For purposes of computation, the free slack of a job is defined as the difference between the job's EF time and the earliest of the ES times of all its immediate successors.

When a job has zero total slack, its scheduled start time is automatically fixed (i.e., ES + LS); and to delay the calculated start time is to delay the whole project. Jobs with positive total slack, however, allow the scheduler some discretion in establishing their start times. This flexibility can usefully be applied to smoothing work schedules.

Peak load may be relieved by shifting jobs on the peak days to their late starts. Slack allows this kind of juggling without affecting project time.

Possible Data Errors in PERT

- The estimated job time may be in error.
- The predecessor relationship may contain cycle errors (job a is a predecessor for b, b is a predecessor for c, and c is a predecessor for a).
- The list of prerequisites for a job may include more than the immediate prerequisites (e.g., job a is a predecessor of b, b is a predecessor of c, and a and b both are predecessor of c).
- Some predecessor relationships may be overlooked.
- Some predecessor relationships listed may be spurious.
- The errors in the PERT calculated project's mean and standard deviation will tend to be large if many noncritical paths each have a duration approximately equal to the duration of the critical path. However, the more slack time there is in each of the noncritical paths, the smaller will be the error.

One way to minimize errors and omissions is to continually back-check the data and challenge the assumptions. Exhibit 5.75 presents advantages and limitations of PERT.

Advantages of PERT	Limitations of PERT
Greatly improved control over complex development work and production programs.	Little interconnection between the different activities pursued.
Ability to distill large amounts of data in brief, orderly fashion.	Requires constant updating and reanalysis of schedules and activities.
Requires a great deal of planning to create a valid network.	Requires greater amount of detail work.
Represents the advent of the management-by-exception principle.	Does not contain quantity information; only time information is available.
People in different locations can relate their efforts to the total task requirements of a large program.	
"Downstream" savings are achieved by earlier and more positive action on the part of management in early project stages.	

EXHIBIT 5.75 Advantages and Limitations of PERT

The following list provides issues that should be considered during PERT implementation.

PERT Implementation Issues

- The people and organization of a project are more important considerations than the use of a particular planning and control technique.

- Consideration should be given to managerial issues, such as project organization, personalities of project members, and operating schemes.
- There is a big difference between the criteria of success for the task to be accomplished and the criteria of success for the management system.
- The project manager is a miniature general manager. However, he or she usually lacks commensurate authority and depends on various management techniques to carry out his or her job.
- The project management approach is the preferred method to deal with onetime defined projects.
- The qualifications of a person making time estimates must include a thorough understanding of the work to be done.
- Precise knowledge of the task sequencing is required or planned in the performance of activities.

APPLICATION OF PERT

Example 1

The network in Exhibit A describes the interrelationships of several activities necessary to complete a project. The arrows represent the activities. The numbers above the arrows indicate the number of weeks required to complete each activity.

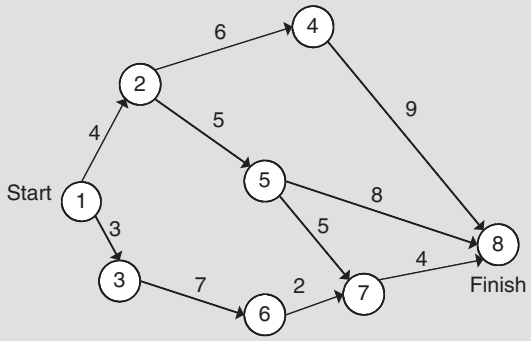


EXHIBIT A PERT Network

Question: What is the shortest time to complete the project?

Answer: The longest path from node (1) to node (8) is path 1–2–4–8. Since all other paths are shorter in duration than path 1–2–4–8, the activities along those paths can be completed before the activities along path 1–2–4–8. Therefore, the amount of time to complete the activities along path 1–2–4–8, which is 19 weeks (4+6+9), is the shortest time to complete the project.

Question: What is the critical path for the project?

Answer: The critical path is the sequence of activities that constrains the total completion time of the project. The entire project cannot be completed until all the activities on the critical path (the longest path) are completed.

Path 1–2–4–8, which takes 19 weeks, is the critical path. Activities along each of the other three paths can be completed (each requires less than 19 weeks) before the activities along 1–2–4–8 can. The other three paths are: 1–2–5–8 (requires 4 + 5 + 8 = 17 weeks), 1–2–5–7–8 (requires 4 + 5 + 5 + 4 = 18 weeks), and 1–3–6–7–8 (requires 3 + 7 + 2 + 4 = 16 weeks).

Example 2

During an operational audit, an internal auditing team discovers the following document, titled Project Analysis.

Project Analysis

Activity	*Time in weeks*	*Preceding activity*
A	3	—
B	3	A
C	7	A
D	4	A
E	2	B
F	4	B
G	1	C, E
H	5	D

Using the Project Analysis document, the audit supervisor prepares the PERT diagram shown in Exhibit B.

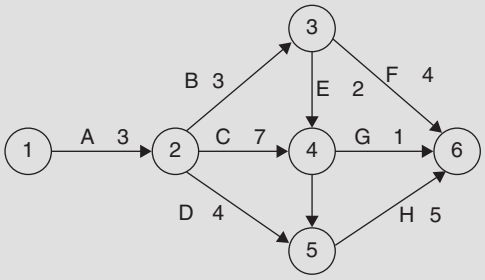


EXHIBIT B PERT Project Analysis

Question: What is the earliest completion time that is indicated by the project analysis?

Answer: There are three paths.

Path 1	A–B–F	=	3 + 3 + 4	=	10 weeks
Path 2	A–C–G	=	3 + 7 + 1	=	11 weeks
Path 3	A–D–H	=	3 + 4 + 5	=	12 weeks

Path 3 has the earliest completion time of 12 weeks since it has the longest time to complete.

Question: What is the earliest time by which Node 4 would be reached?

Answer: There are two paths by which Node 4 can be reached.

Path A	A–C	=	3 + 7	=	10 weeks
Path B	A–B–E	=	3 + 3 + 2	=	8 weeks

Path A has the earliest time of 10 weeks to reach the Node 4 since it has the longest time.

PERT Cost Once the network has been established, based on the project work breakdown structure, costs can be estimated. If the breakdown has been made satisfactorily, it will serve as both an estimating and actual cost accumulation vehicle. PERT cost adds the consideration of resource costs to the schedule produced by the PERT procedure. *The basic PERT handles the problem of time uncertainty while PERT cost addresses cost uncertainty.* Cost uncertainty as it relates to time can be handled by different cost estimates for three time differences. The ultimate objective is not only to improve planning and control but also to assess possibilities for trading off time and cost (i.e., adding or subtracting from one at the expense of the other).

There is an optimum time–cost point for any activity or job as indicated by the U shape of the curve drawn between total direct cost (on *y*-axis) versus time (on *x*-axis). It is assumed that total costs will increase with any effort to accelerate or delay the job away from this point in the case where resource application varies. Crashing the project involves shortening the critical path or paths by operating on those activities that have the lowest time–cost slopes.

At least three approaches are available to develop the cost estimates.

- A singe cost estimate of expected cost
- Three cost estimates
- Optimum time–cost curves

A **single cost estimate** of expected cost is based on the summation of the individual cost elements. The three-cost estimate approach determines the expected cost. The advantage of the **three-cost estimate** over the single-cost estimate is that the result is subject to probability analysis. With this expected cost, the manager cannot assume that he or she has the optimum time–cost mix.

The third approach to estimate is the **optimum time–cost curve concept**. This is differential costing with time as the variability factor. The intention of this approach is to optimize time and costs by using optimum estimated costs. It assumes there is a direct relationship between time and costs on any activity. This relationship can be expressed by a continuous curve. This method is also based on the concept that activities are subject to time–cost trade-offs. The optimum time–cost curve method is difficult to put into practice due to the need to develop continuous time–cost curves.

(B) Critical Path Method The CPM is a powerful but basically simple technique for analyzing, planning, and scheduling large, complex projects. In essence, the tool provides a means of determining which jobs or activities, of the many that comprise a project, are critical in their effect on total project time, and how best to schedule all jobs in the project in order to meet a target date at minimum cost. CPM is an extension of PERT.

Characteristics of Project for Analysis by CPM

- The project consists of a well-defined collection of jobs or activities that, when completed, mark the end of the project.
- The jobs may be started and stopped independently of each other, within a given sequence.
- The jobs are ordered in a technological sequence (e.g., the foundation of a house must be constructed before the walls are erected).

CPM focuses attention on those jobs that are critical to the project time. It provides an easy way to determine the effects of shortening various jobs in the project. It also enables the project manager to evaluate the costs of a crash program.

NORMAL TIME AND CRASH TIME

Time estimates for both normal and crash options are used in the CPM method. Crash time is the time required by the path if maximum effort and resources are diverted to the task along this path. A balance can be obtained when a project manager knows what the normal time and the crash time would be.

It is a costly practice to crash all jobs in a project in order to reduce total project time. If some way is found to shorten one or more of the critical jobs, then not only will the whole project time be shortened but the critical path itself may shift and some previously noncritical jobs may become critical. It is physically possible to shorten the time required by critical jobs by: assigning more people to the jobs; working overtime; and using different equipment, materials, and technology.

When CPM is used in a project to develop a crashing strategy, two or more paths through the network may have nearly the same length. If the activity duration is allowed to vary, a decrease in the length of the critical path may not result in an equivalent decrease in the project duration because of the variance inherent in the parallel or alternate paths. These variations of activity times can even allow the alternate path to become a critical path. Thus, simply allowing the activity times to vary slightly from their estimates in order to make the length of the paths different can cause serious errors in a CPM crashing strategy and lead to wasted resources and cost overruns.

Characteristics of CPM Networks Characteristics of CPM networks are defined next.

- CPM networks attempt to build the entire project on paper at a very early stage of the project—even when the scope is not defined, vaguely defined, or incorrectly defined. In a way, CPM is to project management what modeling or simulation is to economic studies, production problems, plant design, and transportation problems.
- CPM provides a graphic view of the entire project with completion dates, support activities, and costs affixed to every stage of the project.

VALUE OF THE CRITICAL PATH TECHNIQUES

Critical path techniques are as valuable on short- and middle-range planning jobs as they are on major and extremely complex projects.

- CPM's single time estimate fails to consider the effects of variability in path-completion times on the crashing strategy.
- The CPM chart is an excellent tool for communicating scope as well as details of the job to other persons directly and indirectly concerned with the development and completion of the job's various phases.
- The CPM chart serves as a permanent record and reminder of the substance of this communication to all management levels.

- The CPM chart shows the timing of management decisions.
- CPM enables the manager to measure progress (or lack of it) against plans and to take appropriate action quickly when needed. The underlying simplicity of CPM and its ability to focus attention on crucial problem areas of large projects makes it an ideal tool for the senior manager.

CPM versus PERT CPM and PERT methods are essentially similar in general approach and have much in common. However, important differences in implementation details exist. The two methods were independently derived and based on different concepts. Both techniques define the duration of a project and the relationships among the project's component activities. An important feature of the PERT approach is its statistical treatment of the uncertainty in activity time estimates, which involves the collection of three separate time estimates and the calculation of probability estimates of meeting specified schedule dates.

CPM differs from PERT in two areas.

1. The use of only one time estimate for each activity (and thus no statistical treatment of uncertainty)
2. The inclusion, as an integral part of the overall scheme, of a procedure for time/cost trade-off to minimize the sum of direct and indirect project costs

Common Features of PERT and CPM

- They both use a network diagram for project representation, in which diagram circles represent activities with arrows indicating precedence.
- They both calculate early and late start and finish times and slack time.

Exhibit 5.76 provides a comparison of CPM and PERT.

CPM	PERT
CPM uses a single deterministic time estimate to emphasize minimum project costs while minimizing consideration of time restraints. It is the choice of cost-conscious managers.	PERT uses three time estimates to define a probabilistic distribution of activity times that emphasizes minimum project duration while minimizing consideration of cost restraints. It tends to be used by time-conscious managers.

EXHIBIT 5.76 Comparison of CPM and PERT

Although these two techniques are based on different assumptions, they are related to each other because of the obvious relationship between time and cost. The ideal network technique would combine the concepts of CPM's crashing strategy with PERT's probability distribution of activity times to derive the optimum project duration and cost.

(C) Line-of-Balance Technique Line-of-balance (LOB) is a basic tool of project management and was an early forerunner of PERT and CPM. LOB was not as popular as was PERT and CPM. The most successful applications involve methods such as CPM and PERT, which combine simplicity and clarity. These are managerial tools involving planning, scheduling, and control. CPM and PERT require complicated mathematical models while LOB does not.

SCOPE OF LOB TECHNIQUE

- LOB can be performed manually and can be used on large production jobs, maintenance jobs, R&D jobs, and construction jobs.
- LOB requires little training.
- Complex, large-scale LOB problems may require a computer to solve.

LOB is a dynamic managerial tool that can show, at a glance, what is wrong with the progress of a project. It can also point to future bottlenecks. The tool is easy to develop and maintain, manually or by computer and requires no equations or models. It forces the manager to make a plan for the program's completion, and it presents graphical information that sometimes is overlooked in a large volume of data. It does not attempt to optimize operations, but it is a sound basic tool.

The main purpose of the LOB method is to prepare a progress study on critical operations at given times during the actual progress of the job. Each operation is checked against some target; that is, we find where each operation is with respect to where it ought to be. Operations that fall short of target are pointed out for further analysis. LOB uses the principles of management by exception. *LOB allows the manager to pay special attention only to those activities that are both critical and do not conform to the schedule.*

The LOB technique involves four steps.

1. Develop an objective chart or delivery schedule.
2. Prepare a program chart or plan of operation.
3. Develop a progress chart including the LOB.
4. Perform the analysis.

The **objective chart** presents the cumulative delivery schedule of finished goods or services for the entire project in a graphical form. The LOB is graphically derived from the objective chart. It can also be calculated analytically, manually, or by computer.

The **program chart** is best constructed by working backward, starting with the delivery of the finished product as lead time zero. It will show the schedule of each of the critical operations with completion dates and the source and/or responsibility for each operation.

The **progress chart** is a flow process with all critical operations performed from receipt of raw materials to completion.

The objective chart and the program chart are constructed only once. The progress charts must be developed from scratch each time the project is analyzed. The progress chart is therefore good only for a specified date. The core of LOB is **performing analysis** of the progress chart. The analysis pinpoints out-of-balance operations. *It is customary to draw the objective chart, the program chart, and the progress chart on one sheet to get a big, quick picture of the entire project.*

LOB and PERT/CPM are complementary, although each can be used effectively by itself. The distinction between them is that PERT is primarily a planning and evaluation tool for one-unit

type projects, such as R&D with one completion date. PERT's major objective is to identify critical operations, but it can also be used as a control tool by pinpointing deviations from actual performance and rescheduling accordingly.

LOB monitors a project involving many units to be shipped at certain intervals. LOB can also be used in large projects with one completion date. LOB deals both with operations and components and inventories. PERT deals with only one unit and its critical operations. PERT in general requires a computer while LOB is essentially a graphic, manual tool.

LOB and PERT are related to each other. LOB can complement PERT in this way: Once the critical path has been identified, it can be used as part of the program or the production plan of LOB. Other thinking is that these two techniques can be integrated into a single management planning and control system that can be employed from planning stages through production and delivery for a given quantity of items.

Major assumptions of LOB include: The production method is independent of quantities, critical operations do not change with time, and lead time is constant or known with certainty. These assumptions can be related, making the LOB method more complex.

Reasons for low popularity of LOB:

- Lack of awareness of the technique and its potential applicability and advantages
- Management skepticism, which is common to all new managerial techniques
- The lack of a canned computer program for LOB
- Lack of a sound delivery forecast, which is necessary and which is difficult to obtain, considering the difficulty of obtaining market demand and supply forecast
- Requires deterministic lead times (i.e., a single estimate) when, in fact, a range is better

PERT VERSUS CPM VERSUS LOB

- PERT considers time domain only.
- CPM considers cost information only.
- LOB considers quantity information only.
- PERT is good for production prototype construction, assembly, and test of final production equipment that are still high on the learning curve.
- PERT can be applied to smaller projects, single projects, large projects, and multiple projects.
- PERT, CPM, and LOB can be integrated to get maximum benefits.

(D) Graphical Evaluation and Review Technique The graphical evaluation and review technique (GERT) system permits the modeling of a wide variety of situations not possible with traditional PERT/CPM models. Simulation programs can be used to implement GERT, since it uses stochastic networks (i.e., networks in which certain arcs, representing activities, have designated probabilities of occurrence]. GERT allows the performance of alternative, mutually exclusive activities, which are not allowed in the PERT/CPM method. In GERT, activity performance times can be expressed as probability distributions. Heuristic sequencing rules are used to give good resource-feasible schedules.

(E) Work Breakdown Structure The work breakdown structure (WBS) was first intended as the common link between schedules and costs in PERT cost application. Later it became an important tool for conceptual organization of any project. The WBS provides the necessary logic and formalization of task statements. The WBS prepares the work packages, which usually represent the lowest division of the end items.

(F) Gantt Chart The Gantt chart is a bar chart that is essentially a column chart on its side, and is used for the same purpose. The horizontal bar chart is a tool that allows a manager to evaluate whether existing resources can handle work demand or whether activities should be postponed. The Gantt chart is used for milestone scheduling where each milestone has a start and completion date. A milestone represents a major activity or task to be accomplished (e.g., a design phase in a computer system development project).

The Gantt chart is a graphical illustration of a scheduling technique. The structure of the chart shows output plotted against units of time. It does not include cost information. It highlights activities over the life of a project and contrasts actual times with projected times. It gives a quick picture of a project's progress in regard to the status of actual time lines and projected time lines. Exhibit 5.77 presents advantages and disadvantages of PERT and Gantt charts.

Advantages	
PERT	**Gantt chart**
A good planning aid.	A good planning tool.
Interdependencies between activities can be shown.	A graphical scheduling technique that is simple to develop, use, and understand.
Network diagram is flexible to change.	Useful for large projects.
Activity times are probabilistic.	Shows a sequence of steps or tasks.
A good scheduling tool for large, nonroutine projects.	Actual completion times can be compared with planned times.
A good tool in predicting resource needs, problem areas, and impact of delays on project completion.	
Disadvantages	
PERT	**Gantt chart**
Difficult to apply to repetitive assembly-line operations where scheduling is dependent on the pace of machines.	Interrelationships among activities are not shown on the chart.
Large and complex projects are difficult to draw manually.	Inflexible to change.
Requires computer hardware and software to draw a complex network.	Activity times are deterministic.
Requires training to use the computer program.	Difficult to show very complex situations.
	Cannot be used as a procedure documenting tool.
	Does not show the critical path in a chain of activities.

EXHIBIT 5.77 Advantages and Disadvantages of PERT and Gantt charts

WHAT ARE SOPHISTICATED TECHNIQUES FOR PROJECT MANAGEMENT?

- PERT, GERT, and CPM techniques are more sophisticated scheduling methods due, in part, to the consideration of probabilities.
- LOB, WBS, Gantt charts, bar charts, and milestones are less sophisticated scheduling methods due, in part, to not considering the probabilities.
- GERT handles alternate, mutually exclusive activities, while PERT/CPM cannot.

There may be a lower probability of a cost/schedule overrun if PERT is used because of its sophistication as a scheduling method compared to less sophisticated scheduling methods such as Gantt charts, milestone scheduling, line of balance, and bar charts. If there is a slack time, there is no need to use sophisticated and tight scheduling methods, such as PERT.

(vi) Project Controlling Methods

In any project, at least four major types of controls will be applied: (1) time control, (2) cost control, (3) quality control, and (4) earned value management (EVM) control. Sometimes other types of controls are also used (e.g., logs, checklists, and status reports).

Time control. Project network scheduling begins with the construction of a diagram that reflects the interdependencies and time requirements of the individual tasks that make up a project. It calls for work plans prepared in advance of the project. Once the overall schedule is established, weekly or biweekly review meetings should be held to check progress against schedule. Control must be rigorous, especially at the start, so that missed commitments call for immediate corrective action.

Cost control. Periodic reports showing the budget, the actual cost, and variances is a good start for cost controls. It is necessary to break the comprehensive cost summary reports into work packages or major tasks and focus on major problems and opportunities. The cost reports should be distributed to technical as well as functional managers.

Quality control. Quality control comprises three elements: defining performance criteria, expressing the project objective in terms of quality standards, and monitoring progress toward these standards. Examples of performance criteria include market penetration of a product line and processing time for customer inquiries. Both quantitative and qualitative measures need to be defined

EVM control. EVM control provides a standard means of objectively measuring work accomplished based on the budgeted value of that work—it is what you got for what it cost. EVM is a project management technique that integrates cost, schedule, and technical performance measures to monitor and control project resources and compile results into one set of metrics so that effective comparisons can be made. It also helps evaluate and control project risk by measuring project progress in monetary terms. It provides the project manager with a more complete picture of the health of the entire project, not just certain segments of the project.

EVM incorporates three vital aspects of effective project/program management: scoping, costing, and scheduling. EVM is a technique aimed at comparing resource planning to schedules and to technical, cost, and schedule requirements.

The EVM technique serves two distinct purposes: It encourages the effective use of internal cost and schedule management systems, and it affords the organization the ability to rely on timely data produced by those systems for determining product-oriented contracts status. In order to perform an EVM analysis, you need to start with a solid baseline schedule that accurately reflects how much work is planned for each time period. After this baseline is determined and captured, work becomes earned in some quantitative form as work is performed. This earned work is then compared to the initial resource allocation estimates in order to determine if the project or investment has utilized its resources meaningfully and cost efficiently.

Example of Application of EVM Technique

Schedule and Cost Variances

The percentage complete estimate method allows the project manager in charge of the work package to make a monthly or quarterly estimate of the percentage of completed work. These estimates are expressed as cumulative values against 100% of the milestone value. The earned value is then calculated by applying that percentage to the total budget for that work package.

Project A is authorized with a budget of $1,000,000 over a four-quarter, one-year time period. The planned value for the first quarter called for an accomplishment of 30%, or $300,000 (0.30 × $1,000,000) in the value of the work scheduled. Actual costs are amounted to $250,000. The earned value estimate based on 20% of work completed, or $200,000 (i.e., 0.20 × $1,000,000).

Schedule variance = Earned value – Planned value = $200,000 – $300,000 = –$100,000
(i.e., a negative amount means the project is behind schedule)

Cost variance = Earned value – Actual costs = $200,000 – $250,000 = –$50,000
(i.e., a negative amount means the project is experiencing a cost overrun)

Schedule and Cost Performance Indices

Schedule performance index (SPI) = Earned value/Planned value = $200,000/$300,000 = 0.67

Cost performance index (CPI) = Earned value/Actual costs = $200,000/$250,000 = 0.80

A project with SPI and CPI of 1.0 is better, less than 1.0 is not good, and the largest negative value should be given a top priority to work on first.

Forecast of Final Project Costs

A range of final cost requirements can be forcast for the project A using the SPI and CPI indices as follows:

Low-end forecast is Total budget value/SPI = $1,000,000/0.67 = $1,492,537
= $1.5 million (approximately)

High-end forecast is Total budget value/(SPI × CPI) = $1,000,000/(0.67 × 0.80)
= $1,000,000/0.536 = $1,865,672
= $1.9 million (approximately).

A range of final cost projection between a minimum of $1.5 million and a maximum of $1.9 million is needed to complete the project A.

EVM is most effective when implemented using a bottom-up approach. Such an approach dictates that information is planned and managed in small increments that can be quickly and accurately cumulated to view and manages the project as a whole. Examining small, manageable chunks is a more efficient process for identifying problems and root causes, and allows the project manager to assess the health and risks of a project more accurately. Generally, small milestones are easier

to plan for (their scope can be defined more specifically) and can be measured more objectively than large ones. Project managers should ensure that milestones (or submilestones) are as small and specific as possible in terms of scheduling. It is good to limit milestone duration to a single fiscal year (or less), instead of multiyear milestones.

Other types of project controls. Since a project can have a number of people working on it for a long time, monitoring and control become essential management tools. Formal control techniques include" (1) change-management policy, procedures, and forms; (2) logs; (3) checklists; and (4) status reports. Phone conversations and face-to-face communications are some examples of informal control techniques. Where possible, formal control techniques should be practiced, since they provide some evidence as to what has been said and when to resolve a question or dispute.

(vii) Project Governance Mechanisms

Project governance mechanisms include establishing a project steering committee and project oversight board and conducting a project management audit.

The *project steering committee* is a high-level committee to integrate several functions of the organization. The *project oversight board* is similar to steering committee except that it is focused on a specific project at hand. The board:

1. Reviews the project request and scope.
2. Assesses the project impact.
3. Approves the project funding.
4. Challenges the costs, schedules, and benefits.
5. Monitors the project progress.
6. Reviews project deliverables.
7. Solves the project-related problems.

Regarding the project scope, the board determines what is in scope and what is out of scope so that scope creep does not happen. Any changes in project scope are controlled by change management procedures.

(viii) Project Management Audit

The scope of *project management audit* consists of reviewing project planning, organizing, staffing, leading; controlling tasks for effectiveness and efficiency; and determining whether the project objectives and goals are achieved.

The major objective of the project management process, which is part of the software assurance process, is to establish the organizational structure of the project and assign responsibilities. The process uses the system requirements documentation and information about the purpose of the software, criticality of the software, required deliverables, and available time and other resources to plan and manage the software development and maintenance processes. The project management process begins before software development starts and ends when its objectives have been met. The project management process overlaps and often reiterates other software assurance processes. It establishes/approves standards, implements monitoring and reporting practices, develops high-level policy for quality, and cites laws and regulations for compliance.

(A) Review the next 10 activities performed by the project manager in the project planning area.

1. Set objectives or goals; determine the desired outcome for the project:
   - **a.** Analyze and document the system and software requirements; define the relationships between the system and software activities.
   - **b.** Determine management requirements and constraints (resource and schedule limitations)
   - **c.** Define success criteria; always includes delivery of software that satisfies the requirements, on time and within budget.
2. Plan for corrective action.
3. Develop project strategies—decide on major organizational goals (e.g., quality), and develop a general program of action for reaching those goals.
4. Develop policies for the project—make standing decision on important recurring matters to provide a guide for decision making.
5. Determine possible courses of action—develop and analyze different ways to conduct the project; anticipate possible adverse events and project areas; state assumptions; develop contingency plans; predict results, possible courses of action.
6. Make planning decisions—evaluate and select a course of action from among alternatives. This includes:
   - **a.** Choosing the most appropriate course of action for meeting project goals and objectives.
   - **b.** Making trade-off decisions involving costs, schedule, quality, design strategies, and risks.
   - **c.** Selecting methods, tools, and techniques (both technical and managerial) by which the output and final product will be developed and assured and the project will be managed.
7. Set procedures and rules for the project—establish methods, guides, and limits for accomplishing the project activities.
8. Select scheduling process appropriate for development and maintenance methods.
9. Prepare budgets—allocate estimated costs (based on project size, schedule, staff) to project functions, activities, and tasks, and determine necessary resources.
10. Document, distribute, and update project plans.

(B) Review the next six activities performed by the project manager in the project organizing area.

1. Identify and group required tasks—tasks are grouped into logical entities (e.g., analysis tasks, design tasks, coding tasks, test tasks) and are mapped into organizational entities.
2. Select and establish organizational structures—define how the project will be organized (e.g., line, staff, or matrix organization) using contractual requirements and principles of independent verification and validation.
3. Create organizational positions—specify job titles and position descriptions.

4. Define responsibilities and authorities—decide who will have the responsibility of completing tasks and who has the authority to make decisions related to the project.
5. Establish position qualifications—identify the qualities personnel must have to work on the project (e.g., experience, education, programming languages, tool usage).
6. Document organizational structures—document lines of authority, tasks, and responsibilities in the project plan.

(C) Review the next eight activities performed by the project manager in the project staffing area.

1. Fill organizational positions—fill the jobs established during organizational planning with qualified personnel.
2. Assimilate newly assigned personnel—familiarize newly assigned personnel with any project procedures, facilities, equipment, tools, or plans.
3. Educate and train personnel as necessary.
4. Provide for general development of project staff members.
5. Evaluate and appraise personnel.
6. Compensate project personnel (e.g., salary, bonus).
7. Terminate project assignments—reassign or terminate personnel at the end of a project.
8. Document staffing decisions—document staffing plans, training policies adopted.

(D) Review the next seven activities performed by the project manager in a project leading area.

1. Provide leadership—the project manager provides direction to project members by interpreting plans and requirements.
2. Delegate project authority.
3. Build project teams.
4. Coordinate and communicate project activities between in-house and contractor personnel.
5. Resolve project conflicts.
6. Manage changes after considering the inputs, outputs, costs/benefits.
7. Document directing decisions taken.

(E) Review the next five activities performed by the project manager in the project controlling area.

1. Develop standards of performance—select or approve standards to be used for the software development and maintenance activities.
2. Establish monitoring and reporting systems, such as milestones, deliverables, schedules.
3. Analyze results by comparing achievements with standards, goals, and plans.
4. Apply corrective action to bring requirements, plans, and actual project status into conformance.
5. Document the controlling methods used.

(b) Change Management Methods

(i) Agents of Change

Organizations must change to survive in a competitive environment. This requires everyone in the organization believing in and accepting the change. Ideally, managers need to be architects or agents of change rather than the victims of change. When introducing changes, managers often are surprised that things do not turn out as planned. This is because the change process is not carried out properly. The change itself is not the problem. When managers are acting as agents of change, their company will be much more responsive, flexible, and competitive. In addition to managers, internal auditors can act as change agents due to their nature of work. Auditors facilitate change through their recommendations to management. Each recommendation auditors make requires some change in existing policies, procedures, and practices or creation of new ones.

(ii) How to Change

A corporation can change in a number of ways. These include:

- Reengineering business policies, processes, jobs, and procedures; outsourcing nonstrategic activities.
- Partnering with major suppliers and customers.
- Implementing TQM programs.
- Redesigning the organizational structure to fit the business strategy.
- Renovating physical plants and facilities.
- Installing computer-based systems and technologies.
- Understanding its own products, services, markets, and customers and those of competitors.
- Installing performance measurement methods and reward systems.

PROMOTERS VERSUS RESISTORS OF CHANGE

People at the top of the organization usually promote change because they have clear vision and better goals to achieve.

People at the bottom of the organization usually resist change the **least** because they know how bad things really are at their level.

People at the middle of the organization usually resist change the **most** because they know neither top management goals nor how bad things really are at the bottom. They are in a confused stage since they know neither the top nor the bottom.

(iii) Types of Organizational Change

Organization psychologists David Nadler and Michael Tushman developed an instructive typology of organizational change describing four types of changes (see Exhibit 5.78).[35]

[35] Kreitner, *Management.*

	Incremental	Strategic
Anticipatory	Tuning 1	Reorientation 3
Reactive	Adaptation 2	Re-creation 4

EXHIBIT 5.78 Typology of Organizational Change

As the exhibit shows, **anticipatory changes** are any systematically planned changes intended to take advantage of expected situations (e.g., following demographics). **Reactive changes** are those necessitated by unexpected environmental events (e.g., responding to competitor's action). **Incremental changes** involve the subsystems adjustments needed to keep the organization on its chosen path (e.g., adding a third shift in a manufacturing plant). **Strategic changes** alter the overall shape or direction of the organization (e.g., switch from building houses to apartments by a construction contractor).

The four specific resulting types of organizational change from the previous exhibit are tuning, adaptation, reorientation, and re-creation (see Exhibit 5.79).

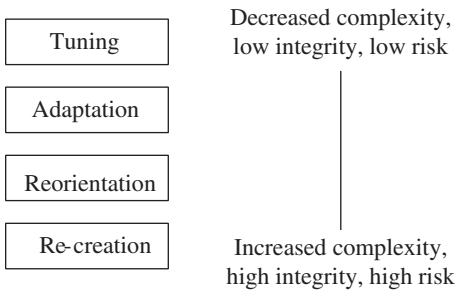


EXHIBIT 5.79 Specific Types of Organizational Change

In this exhibit, **tuning** is the most common form of organizational change covering preventive maintenance and continuous improvement. The major thrust of tuning is to actively anticipate and avoid problems rather than passively waiting for things to go wrong before taking action. *Managers should seek change, not just expect change.*

Adaptation, like tuning, involves incremental changes. The difference is that the changes are in reaction to external problems, events, or pressures. The **reorientation** change is anticipatory and strategic in scope. It is also called frame bending because the organization is significantly redirected while continuing its original mission. **Re-creation** is a type of change that is reactive and strategic in scope. It is also called frame breaking because the new organization is completely different from the organization of the past.

(iv) Resistance to Change

Organizational change comes in all forms, sizes, and shapes and with various degrees of impacts and consequences for employees. Some of the most common reasons for resistance to change are listed next.

- Surprise
- Inertia

- Misunderstanding
- Emotional side effects
- Lack of trust
- Fear of failure
- Personality conflicts
- Lack of tact
- Threat to job status or security
- Breakup of work groups

Management faces the challenge of foreseeing and neutralizing resistance to change, as the resistance is both rational and irrational.

Management theorists have offered at least six options to overcome resistance to change:

1. Education and communication
2. Participation and involvement
3. Facilitation and support
4. Negotiation and agreement
5. Manipulation and co-optation
6. Explicit and implicit coercion

Situational appropriateness is the key to success.

- **Education and communication.** This option promotes prevention rather than cure. The idea here is to help employees understand the true need for a change as well as the logic behind it. Various media may be used, including face-to-face discussions, formal group presentations, and special reports or publications. *Advantages:* Once persuaded, employees will help with the implementation of the change. *Drawbacks:* Education and communication can be time consuming if many employees are involved.
- **Participation and involvement.** Personal involvement through participation tends to defuse rational and irrational fears about a workplace change. Involvement in the design and implementation of a change makes one become an owner of the change process and its success. *Advantages:* Participation and involvement lead to commitment from employees. *Drawbacks:* Participation and involvement can be time consuming if participators design an inappropriate change.
- **Facilitation and support.** Support from management in the form of special training, job stress counseling, and compensatory time off can be helpful when fear and anxiety are responsible for resistance to change. *Advantages:* No other approach works as well with adjustment problems. *Drawbacks:* Facilitation and support can be time consuming, expensive, and still fail.
- **Negotiation and agreement.** Management can neutralize resistance to change by exchanging something of value for cooperation. *Advantages:* It is a relatively easy way to avoid major resistance. *Drawbacks:* Negotiation and agreement can be too expensive in many cases if others are alerted to negotiate for compliance.

- **Manipulation and co-optation.** Manipulation occurs when managers selectively withhold or dispense information and consciously arrange events to increase the chance that a change will be successful. Co-optation normally involves token participation, of employees and the impact of their input is negligible. *Advantages:* It can be a relatively quick and inexpensive solution to resistance problems. *Drawbacks:* The process can lead to future problems if people feel manipulated.
- **Explicit and implicit coercion.** Managers who cannot or will not invest the time required for the other strategies can force employees to go along with a change by threatening them with termination, loss of pay raises or promotions, transfer, and so forth. *Advantages:* It is speedy, and can overcome any kind of resistance. *Drawbacks:* This process can be risky if it leaves employees mad at the initiators.

(v) Factors to Consider during the Change Process

Internal auditors should consider the following factors during their audit work:

- A real paradigm shift is needed for changes to take place. Excuses like "It is our company policy" and "We have no resources" no longer work. Forward-looking people are needed.
- Motivating stakeholders (employees, customers, and suppliers) can have a multiplier effect on the change initiative. Their involvement in problem solving and knowledge sharing is vital.
- The active performance measures are not always obvious. They should be made explicit.
- During the change implementation process, expect setbacks and roadblocks. Address them on a case-by-case basis.
- Communicating honestly is important. Act straightforward with all stakeholders.
- Use the grapevine to a project's advantage; do not let the project be abused by it.
- Empower employees so they feel that they have real influence over standards of production, quality, and service. Empowering people brings significant changes in employees' behavior. However, managers who do the empowering must also change. Empowerment means that employees have the correct knowledge and appropriate tools to do things well, not just have the authority to do the job.
- Identify the barriers to change. If possible, dismantle them; at least, deal with them.
- Today's change projects require border crossing of departments, divisions, suppliers, and customers. Borderless projects should be encouraged since border-bound projects like to maintain their own turf.
- A goal-focused and results-oriented performance measurement system is needed to institutionalize the changes since performance measures are a primary strategy deployment tool. Do not settle for a single measurement; instead, opt for a set of measures.
- Understand and consider the cultural differences at the workplace. Do not discount them.

(vi) Organizational Development

Organizational development (OD) is a systematic approach to planned change programs intended to help employees and organizations function more effectively. OD combines the knowledge from various disciplines, such as behavioral science, psychology, sociology, education, and management. OD is a process of fundamental change in an organization's culture. For OD programs to be effective, not only must they be tailored to unique situations, but they also must meet the

seven common objectives in order to develop trust. *Problem-solving skills, communication, and cooperation are required for success.*

1. Deepen the sense of organizational purpose and align individuals with that purpose.
2. Strengthen interpersonal trust, communication, cooperation, and support.
3. Encourage a problem-solving rather than a problem-avoiding approach to organizational problems.
4. Develop a satisfying work experience capable of building enthusiasm.
5. Supplement formal authority with authority based on personal knowledge and skill.
6. Increase personal responsibility for planning and implementing.
7. Encourage personal willingness to change.

Organization development brings out pros and cons.

Pros: General management lacks a systematic approach and is often subject to haphazard, bits-and-pieces management style. OD gives managers a vehicle for systematically introducing change by applying a broad selection of management techniques as a unified and consistent package. This approach leads to greater personal, group, and organizational effectiveness.

Cons: The seven common objectives listed above are not new. They have been addressed by one or another management techniques.

(A) OD Process Social psychologist Kurt Lewin recommended that change agents unfreeze, change, and then refreeze social systems related to three major phases or components of OD.[36]

Unfreezing phase → Change phase → Refreezing phase

Unfreezing involves neutralizing resistance by preparing employees for change. Change involves implementing the change strategy. Refreezing involves systematically following up a change program for permanent results.

(B) Unfreezing Phase The objective of unfreezing phase is to assess the situation and suggest an appropriate change strategy. The scope of work includes making announcements, holding meetings, and launching a promotional campaign in the organization's newsletter and on bulletin boards. The goal is to deliver a clear message to employees about the change. Management needs to avoid creating unrealistic expectations such as miracles.

During the unfreezing phase, management may choose to diagnose the situation by using several approaches, such as:

1. Reviewing records (personnel or financial) for signs of excessive absenteeism, cost overruns, budget variances.
2. Interviewing employees with specific questions about their job and the organization.

[36] Ibid.

3. Mailing survey questionnaires for opinions and suggestions.
4. Observing employees at work, since people tend to say one thing and do another.

After the data are collected and compiled, it is good to compare the results with past results to see how things have changed. This would help in mapping a future course of action.

(C) Change Phase The objective of the change phase is to implement the change strategy through enhanced collaboration and cooperation. In this phase of intervention, the wheels of change are set in motion. "Intervention" here means that a systematic attempt will be made to correct an organizational deficiency uncovered through diagnosis.

Six popular OD interventions designed to increase effectiveness are listed next.

1. Life and career planning
2. Skill development
3. Role analysis
4. Team building
5. Survey feedback
6. Grid OD

These six interventions are grouped into three categories: (1) individual, (2) group, and (3) entire organization targets, as shown in Exhibit 5.80.

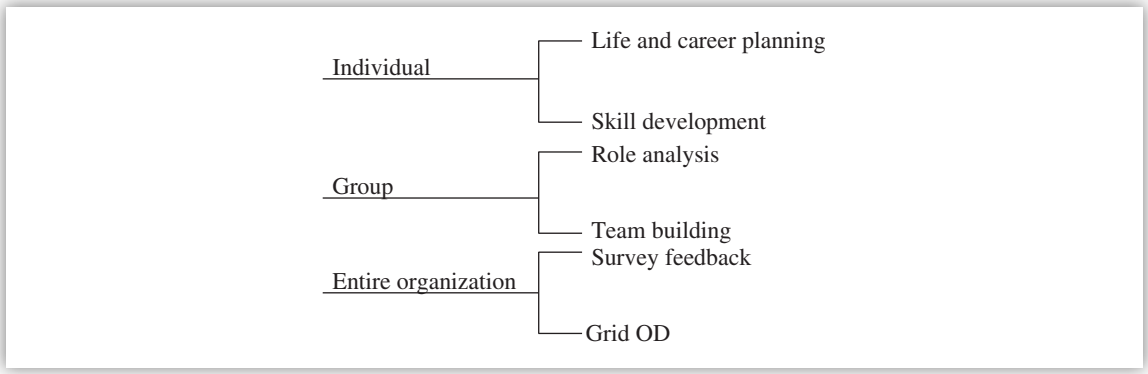


EXHIBIT 5.80 OD Interventions

Individual Interventions The overall objective of *life and career planning* is to get individuals to define their personal goals for growth and development and to plan ways to achieve them. Here an assumption is made that organizational growth and development is a function of individual growth and development. The overall objective of *skill development* is to place emphasis on learning how to do it in terms of delegation, problem solving, conflict resolution, and leading. Skill development deals with content rather than process.

Group Interventions The overall objective of *role analysis* is to define a prescribed way of behaving. A systematic clarification of interdependent task and job behavior is made. The overall

objective of *team building* is to place emphasis on interactive group processes, the "how" of effective group behavior. This intervention is the most widely used HR development technique.

Entire Organization Interventions The overall objective of *survey feedback* is to inform employees where they stand in relation to others on important organizational issues so that constructive problem solving can take place. Effective feedback should be relevant, understandable, descriptive, verifiable, controllable, comparative, and inspiring. The overall objective of *grid OD* is to present a package covering several OD interventions arranged in an orderly and coherent fashion. OD grid is based on Blake and Mouton's leadership grid, a popular OD approach.

(D) Refreezing Phase The objective of the refreezing phase is to address unanticipated problems and side effects and to maintain positive changes. The effectiveness of change strategy is also evaluated. The scope includes follow-up and monitoring to ensure lasting change.

Maintaining Positive Changes The goal is to induce employees to behave differently and positively. This calls for more cooperation, more collaboration, and more productivity among employees. Some of the items for maintaining positive changes include top management support, peer group support, and a formal reward and punishment system, all of which lead to a supportive climate for change on the job.

Evaluating the OD Program An objective evaluation of results is desired even though it is difficult, time consuming, and expensive. According to a recent statistical analysis conducted by Neuman, Edwards, and Raju:[37]

- Combined interventions were more effective at improving employee attitudes and satisfaction than were single-technique interventions.
- Team building was the most effective OD intervention for improving attitudes and satisfaction.
- OD interventions tend to have a stronger influence on attitudes than on satisfaction.
- The empirical linkages between OD interventions and productivity are not strong.

[37] Neuman, Edwards, and Raju, *Personal Psychology* (Autumn 1989).

5.6 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Where does the information about opportunities and threats come from for a company?

a. An analysis of the organization's internal environment

b. A department-by-department study of the organization

c. A scan of the external environments

d. An analysis of employee grievances

2. The costs of providing training and technical support to the supplier in order to increase the quality of purchased materials are examples of:

a. Prevention costs.

b. Appraisal costs.

c. Internal failure costs.

d. External failure costs.

3. All of the following are effective ways to prevent service mistakes from occurring **except**:

a. Source inspections.

b. Self-inspections.

c. Sequence checks.

d. Mass inspections.

4. Which of the following is **not** one of the principles of total quality management (TQM)?

a. Do it right the first time.

b. Strive for zero defects.

c. Be customer centered.

d. Build teamwork and empowerment.

5. Recent events caused the time series used by an electric utility to become too unpredictable for practical use. As a result, the utility developed a model to predict the demand for electricity based on factors such as class of service, population growth, and unemployment in the area of service. The discipline that deals with such models is called:

a. Linear programming.

b. Network analysis.

c. Operations research.

d. Econometrics.

6. A company wishes to forecast from time series data covering 20 periods. Which of the following is **not** an appropriate forecasting technique?

a. Weighted least squares

b. Exponential smoothing

c. Delphi technique

d. Moving average process

7. The auditor has recognized that a problem exists because the organizational unit has been too narrow in its definition of goals. The goals of the unit focus on profits, but the overall organizational goals are much broader. The auditor also recognizes that the auditee will resist any recommendations about adopting broader goals. The best course of action would be to:

a. Avoid conflict and present only those goals that are consistent with the auditee's views since all others will be ignored.

b. Identify the broader organizational goals and present a set of recommendations that attempts to meet both the organizational and auditee goals.

c. Subtly mix the suggested solution with the problem definition so that the auditee will identify the solution apparently independently of the auditor.

d. Only report the conditions found and leave the rest of the analysis to the auditees.

8. Which of the following problem-solving tools is an idea-generating and consensus-building technique?

a. Brainstorming

b. Synectics

c. Systems analysis

d. Nominal group technique

9. Job performance is best defined as follows:

a. Job performance = Motivation × Ability.

b. Job performance = Needs × Skills.

c. Job performance = Satisfaction × Job experience.

d. Job performance = Goals × Training.

10. Individual commitment to groups is based on attractiveness and which of the following?

a. Groupthink

b. Appearance

c. Cohesiveness

d. Conformity

11. "Apple polishing" is done to:

a. Make the supervisor look good.

b. Build an empire.

c. Create cliques.

d. Create destructive competition.

12. Which of the following is a **critical** challenge in implementing employee empowerment principle?

a. Pushing authority downward closer to front-line employees

b. Expecting accountability from all employees

c. Delegating employees with restrictions to achieve objectives

d. Developing clear and complete job descriptions for employees

13. In light of rapidly changing technologies and increasing competition and to provide the ability to affect quality initiatives, which of the following human resources policies and practices is **not** enough?

a. Hiring competent employees

b. Providing one-time training for employees

c. Encouraging continuing education for employees

d. Conducting periodic performance evaluations for employees

14. From a human resources policies and practices viewpoint, which of the following sends a strong message to all interested parties?

a. Expected levels of integrity

b. Expected levels of disciplinary actions

c. Expected levels of ethical behavior

d. Expected levels of competence and trust

15. Commitment falls under which of the following types of a leader's power?

a. Reward power

b. Coercive power

c. Expert power

d. Referent power

16. Which of the following should be done **before** job descriptions are developed?

a. Job analyses

b. Job rotation

c. Job specifications

d. Job matrix

17. Which of the following defines the process of evaluating an individual's contribution as a basis for making objective personnel decisions?

a. Performance appraisal

b. Environmental factors

c. Facilitation skills

d. Training and development

18. Negotiation, manipulation, coercion, employee education, and increased communication are all ways in which managers can:

a. Improve employee morale.

b. Overcome resistance to change.

c. Maintain control of information.

d. Demonstrate their power to both their supervisors and subordinates.

19. The adoption of a new idea or behavior by an organization is known as organizational

a. Development.

b. Change.

c. Structure.

d. Intervention.

20. If top managers select a goal of rapid company growth, which of the following will have to be changed **first** to meet that growth?

a. Competitive actions

b. Internal actions

c. External actions

d. Environmental actions

21. Which of the following is the most common, least intense, and least risky type of change in an organization?

a. Tuning

b. Reorientation

c. Re-creation

d. Adaptation

22. Which of the following strategies for overcoming resistance to change should be used when the concern is prevention?

a. Education and communication

b. Participation and involvement

c. Facilitation and support

d. Negotiation and agreement

23. In project management, each activity has two pairs of durations called:

a. Normal and crash time.

b. Normal and budget time.

c. Actual and crash time.

d. Quantity and quality time.

24. In project management, which of the following measures the cost efficiency with which the project is being performed?

a. Cost variance

b. Schedule variance

c. Schedule performance index

d. Cost performance index

25. In project management, the schedule performance index (SPI) analysis should include identifying those work packages within the project that should be given top priority to work on it **first** is:

a. A negative SPI of 1.0.

b. A positive SPI of 1.0.

c. A negative SPI of 2.0.

d. A positive SPI of 2.0.

DOMAIN 6

Information Technology and Business Continuity (15–25%)

6.1 Security

(a) Information Security Objectives

Security objectives, security controls, security policies, and security impact analysis are presented in this section.

(i) Security Objectives

There are five security objectives: confidentiality, integrity, availability, accountability, and assurance. However, information systems literature focuses primarily on three security objectives or attributes: confidentiality, integrity, and availability. These three objectives (i.e., confidentiality, integrity, and availability) form the three legs of the **CIA triad**. Another definition of security, according to the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 13335 Standard, is that it encompasses all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

1. **Confidentiality.** Confidentiality of data and information is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection in regard to data concerns data in storage, during processing, and while in transit. Confidentiality is the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Thus, confidentiality is related to privacy.
2. **Integrity.** Integrity of system and data is required as protection against intentional or accidental attempts to violate either (a) data integrity—the property that data have not been altered in an unauthorized manner while in storage, during processing, or while

in transit, or (b) system integrity—the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation. In other words, integrity is lack of improper modification, alteration, or destruction.

3. **Availability.** Availability of system and data is a requirement intended to ensure that systems work promptly and service is not denied to authorized users. This objective protects against (a) intentional or accidental attempts to either perform unauthorized deletion of data or otherwise cause a denial of service/data, and (b) attempts to use system or data for unauthorized purposes. Availability means that data are continually and reliably accessible and usable in a timely manner, including the ability to share.
4. **Accountability.** Accountability is the requirement that actions of an entity may be traced uniquely to that entity. Accountability (i.e., taking responsibility for one's own actions and inactions) is dependent on confidentiality and integrity. If confidentiality or integrity is lost, accountability is threatened. Note that availability and accountability share the same concerns and controls. Accountability is often an organizational policy requirement and directly supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action (e.g., audits, investigations, and courts). Here accountability is at the individual level. It is the ability to associate actors with their acts and to include nonrepudiation (i.e., ensuring that actors are unable to deny—repudiate—an action).
5. **Assurance.** Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the data it processes. Assurance verifies that the other four security objectives (i.e., confidentiality, integrity, availability, and accountability) have been adequately met by a specific implementation. Something is "adequately met" when (a) required functionality is present and performs correctly, (b) there is sufficient protection against unintentional errors (by users or software), and (c) there is sufficient resistance to intentional penetration or bypass. Assurance addresses the question of the amount of uncertainty one should have in software system.

When designing an information system, a system architect or system designer should establish an assurance level as a target. This target is achieved by both defining and meeting the functionality requirements in each of the other four security concepts and doing so with sufficient quality. Assurance highlights the fact that for an information system to be secure, it must not only provide the intended functionality but it also must ensure that undesired actions do not occur. Assurance is essential; without it, the other security objectives are not met. However, assurance is a continuum; the amount of assurance needed varies between information systems.

Another view of an information system is that it must be dependable at all times. "Dependable" is a qualitative, umbrella term. Dependability is an integrating concept that encompasses six attributes or properties:

1. Confidentiality
2. Integrity
3. Availability
4. Reliability
5. Safety
6. Maintainability

Although properties such as reliability (i.e., continuity of correct service), safety (i.e., absence of catastrophic consequences on the user and the environment), and maintainability (i.e., the ability to undergo modifications and repairs) may not directly result in secure software, they all contribute to keeping the security up-to-date and showing that the software is secure.

(ii) Security Controls

Access controls fortify the CIA triad by identifying, authenticating, and authorizing users to access systems and data. Poor access controls and inadequate disaster recovery plans can prevent an organization from reasonably ensuring the objectives or goals of the CIA triad.

The interdependencies between the CIA triad and security controls are listed next.

> **Confidentiality** (i.e., sensitivity, criticality, secrecy, nondisclosure, and privacy) is dependent on integrity, in that if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid. Thus, confidentiality is tied to integrity. Implementing the safeguards (controls) suggested in Exhibit 6.1 can help toward achieving the confidentiality objective.

Security Objective	Security Controls
Confidentiality	Use encryption techniques during data/program storage and transmission; use digital signature verification techniques; develop data classification schemes; require all employees sign nondisclosure statements to ensure transaction privacy; implement accountability principle by logging and journaling system activity; implement security policies, procedures, and standards; implement system user identification, authentication, and authorization techniques; implement reference monitor concept in the design of an operating system; implement layers of controls to prevent impersonation and tailgating; implement logical and physical access controls; establish employee security awareness and training programs; establish document and file disposition controls; establish security labels and tags to storage media and data files to reflect their sensitivity; install audit trails and journals to provide transaction monitoring capability; and audit the adequacy of confidentiality safeguards.

EXHIBIT 6.1 Controls to Achieve the Confidentiality Objective

> **Integrity** (i.e., accuracy, authenticity, nonrepudiation, accountability, and completeness) is dependent on confidentiality, in that if the confidentiality of certain information is lost (e.g., due to the use of the superuser password), then the integrity mechanisms are likely to be bypassed. Implementing the safeguards (controls) suggested in Exhibit 6.2 can help toward achieving the integrity objective.
>
> **Availability** (i.e., usability and timeliness) is dependent on confidentiality and integrity, in that (1) if confidentiality is lost for certain information (e.g., superuser password), the mechanisms implementing these objectives are easily bypassable; and (2) if system integrity is lost, then confidence in the validity of the mechanisms implementing these objectives is also lost. Implementing the safeguards (controls) suggested in Exhibit 6.3 can help toward achieving the availability objective.

Security Objective	Security Controls
Integrity	Implement system/user identification, authentication, and authorization techniques; implement logical and physical access controls; use encryption techniques during data/program storage and transmission; use digital signature verification techniques; implement intrusion detection and response programs; install data editing and validation routines for data input, process, and output; install antivirus software; implement security policies, procedures, and standards; implement layers of controls to prevent impersonation and tailgating; establish data reconciliation controls; implement reference monitor concept in the design of an operating system; use disk repair utility programs for PCs; make system and data backups; establish employee security awareness and training programs; implement variance detection techniques in sensitive transaction processing; install audit trails and journaling to provide transaction monitoring capability; audit the adequacy of integrity safeguards.

EXHIBIT 6.2 Controls to Achieve the Integrity Objective

Another way of presenting the security controls is to classify them from a technical viewpoint and according to their action, such as preventive controls, detective controls, and recovery controls. These controls are described next.

- **Preventive controls** focus on inhibiting security breaches from occurring in the first place. They include identification, authentication, authorization, access control enforcement, cryptographic key management, nonrepudiation, system protections, transaction privacy, protected communications, and security administration.
  - **Identification.** This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control, mandatory access control, and accountability), it is essential that both subjects and objects be identifiable. Identification control recognizes an entity (e.g., user, program, device, or process) prior to access.

Security Objective	Security Controls
Availability	Establish software configuration controls; implement disaster recovery and contingency plans; purchase insurance coverage; implement logical and physical access controls; implement user/system authorization mechanisms; implement intrusion detection and response programs; implement records management programs; install asset management system for tracking software and hardware inventory; implement logical and physical access controls; make system and data backups; use loosely coupled parallel processor architecture for fail-safe operation; implement incident logging and reporting; install fault-tolerant hardware and software for continuous operation; require extra power supplies and cooling fans; establish employee security awareness and training programs; conduct computer capacity planning; implement redundancy and recovery features; and audit the adequacy of availability safeguards.

EXHIBIT 6.3 Controls to Achieve the Availability Objective

- **Authentication.** The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Weak authentication mechanisms include passwords and personal identification numbers (PINs). Strong authentication mechanisms include token, smart card, digital certificate, and Kerberos. Authentication often acts as a prerequisite to allowing access to resources in a computer system.
- **Authorization.** The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).
- **Access control enforcement.** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized and validated to access particular computer processes, it is necessary to enforce the defined security policy (i.e., discretionary or mandatory access control). These policy-based access controls are enforced via access control mechanisms distributed throughout the system (e.g., mandatory access control–based sensitivity labels, discretionary access–based control file permission sets, access control lists, roles, file encryption, and user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security). Checking identity and requested access against access control lists (ACLs) and using file encryption methods are examples of access control enforcement mechanisms.

  The correct sequence of access to a computer or information resource is shown next.

  Identification→Authentication→Authorization→Access Control Enforcement

- **Cryptographic key management.** Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. The scope of key management includes key generation, distribution, storage, and maintenance.
- **Nonrepudiation.** System accountability depends on the ability to ensure that senders cannot deny sending data and that receivers cannot deny receiving it. Nonrepudiation control provides an unforgeable proof of sending and/or receiving data, and its scope spans prevention and detection categories. It has been placed into the prevention category because the mechanism implemented prevents the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). Consequently, this control typically is applied at the point of transmission or reception.
- **System protections.** Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective of both the design processes used and of manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (need-to-know), process separation, modularity, layering, abstraction, encryption, data hiding, and minimization of what needs to be trusted.
- **Transaction privacy.** Both government and private-sector systems are increasingly required to maintain the privacy of individuals using the systems. Transaction privacy controls (e.g., secure sockets layer and secure shell) protect against loss of privacy with respect to transactions performed by an individual.

- **Protected communications.** In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network and Internet Protocol security [IPsec] protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, Rivest-Shamir-Adelman (RSA), Message Digest 4 (MD4), MD5, and secure hash standard), and escrowed encryption algorithms (e.g., Clipper) to minimize such network threats as replay, interception, packet sniffing, wiretapping, or eavesdropping. Protected communications must be safe from disclosure, substitution, modification, and replay attacks.
- **Security administration.** The security features of an information technology (IT) system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application system. Commercial off-the-shelf add-on security products are available.

- **Detective controls** focus on detecting security breaches. Specifically, detective controls warn of violations or attempted violations of security policies and procedures. They are needed to complement or supplement the preventive controls because the latter controls are not perfect. Detective controls include audits, audit trails, checksums, intrusion detection and containment, proof of wholeness, and virus detection and eradication.
  - **Audits.** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of and recovery from security breaches. After-the-fact events include audits, investigations, and court evidence.
  - **Audit trails.** Audit trails show a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of events surrounding or leading to an operation, procedure, or event, from beginning to the end. They show who has accessed a system and what operations are carried out in aiding tracing system activities.
  - **Checksums.** Checksums show a value automatically computed on data to detect errors or manipulations during transmission and to ensure the accuracy of data transmission. The number of bits in a data unit is summed and transmitted along with the data. The receiving computer then checks the sum and compares, and any changes are noticed.
  - **Intrusion detection and containment.** It is essential to detect security breaches (e.g., network break-ins and suspicious activities) so that a response can occur in a timely manner.
  - **Proof of wholeness.** The proof-of-wholeness control (e.g., a system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. It determines whether integrity has been compromised and whether information state or system state has been corrupted. However, this control does not prevent violations of security policy; it detects violations and helps determine the types of corrective action needed.
  - **Virus detection and eradication.** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

- **Recovery controls** focus on recovering from security breaches as they restore lost computing resources. Recovery controls are needed as a complement or supplement to preventive controls and detective controls because the latter two types are not perfect. Recovery controls include backups, checkpoints, contingency plans, and controls to restore a system to its secure state.
  - **Backups.** Backup methods copy files and programs to facilitate recovery in a timely manner.
  - **Checkpoints.** Checkpoints provide restore procedures before, during, or after completion of certain transactions or events to ensure acceptable level of fault recovery.
  - **Contingency plans.** Contingency plans provide policies and procedures designed to maintain or restore business operations and computer operations, at the primary processing center and/or at an alternate processing site.
  - **Restore to a secure state.** This control enables a system to return, after a security breach occurs, to a state known to be secure.

(iii) Security Policies

Effective security policies and procedures are the first step or the first line of defense to ensure secure systems and networks. To make the security policy effective, it must be practical and enforceable, and it must be possible to comply with the policy. The policy must not significantly impact productivity, be cost prohibitive, or lack support. This delicate balance is best accomplished by including both functional management and information security management in the policy development process.

The four basic types of security policies that exist—program policy, issue-specific policies, system-specific policies, and acceptable use policies—are discussed next.

1. **Program policy** is used to create an organization's information security program. Contents of program policy include purpose, scope, responsibilities, and compliance (i.e., penalties and disciplinary actions). It contains scope, responsibilities, strategic direction, and resources.
2. **Issue-specific policies** address specific issues of concern to the organization. Examples of specific issues include:
   - Internet access
   - E-mail privacy
   - Approach to risk management and contingency planning
   - Protection of confidential and proprietary information
   - Use of unauthorized software
   - Acquisition of software
   - Doing computer work at home
   - Bringing in disks from outside the workplace
   - Access to other employees' files
   - Encryption of files and e-mail

- Rights of privacy
- Responsibilities for correctness of data
- Suspected malicious code
- Physical emergencies, such as fire and flood

Issue-specific policies cover contingency planning, risk management, and implementation of new regulations or laws.

3. **System-specific policies** focus on decisions taken by management to protect a particular system, such as application systems and network systems (i.e., management controls). Components of system-specific policies include security objectives and operational security rules. System-specific policies are often implemented through the use of logical access controls. They contain access control lists for a specific system, training users, and e-mail/fax security policy. Some examples of system-specific policies, where both functional management and information security management work together to develop, include:
   - Creating a Gold Disk (master disk) in configuration management as a baseline of configurations
   - Developing modem usage policy
   - Developing a wireless security policy for planning, deploying, and configuring wireless access points to prevent war-driving attacks
4. **Acceptable use policies** require that a system user, an end user, or an administrator (e.g., system, security, and network administrator) agrees to comply with such policies prior to accessing computer systems, internal networks, and external networks (the Internet). Acceptable use is based on authorized access. For example, in a cloud computing environment, subscribers ensure that all subscriber personnel read and understand the provider's acceptable use policy and negotiate an agreement for resolution of agreed-on policy violations in advance with the provider. The agreement also includes a process for resolving disputes over possible policy violations.

In addition to security policies, rules of behavior and rules of engagement must be considered to exact proper behavior from employees and from outside contractors and vendors.

The term "rules of behavior" describes the rules established and implemented concerning use of, security in, and acceptable level of risk of the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage.

A rules of behavior document:

- Defines scope of coverage, including work at home; dial-in access; connection to the Internet; use of copyrighted work; unofficial use of organization equipment; assignment and limitations of system privileges and individual accountability in using passwords; searching databases; and divulging information.
- Delineates responsibilities, expected use of system, and behavior of all users
- Describes appropriate limits on interconnections of systems.
- Defines service provisions and restoration priorities.

- Clarifies consequences of behavior not consistent with rules of behavior.
- Provides detailed guidelines and constraints regarding the execution of information security testing.

Rules of Engagement The rules of engagement are established before the start of a security test. The document gives the test team authority to conduct the defined activities without the need for additional permissions. Rules of engagement are aimed at outside contractors and vendors before performing their work for an organization.

(iv) Security Impact Analysis

In an information system, an "impact" is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, unauthorized modification, unauthorized destruction, or loss of information or loss of information system availability.

Impact levels are categorized as high, moderate, or low in regard to the intensity of a potential impact that may occur if the information system is jeopardized or compromised.

- A **high-impact system** is an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high.
- A **moderate-impact system** is an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.
- A **low-impact system** is an information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a potential impact value of low.
- A **potential impact** considers all three levels of impact regarding the loss of confidentiality, integrity, or availability. It could be expected to have a
  - **a.** Limited adverse effect (low);
  - **b.** Serious adverse effect (moderate); or
  - **c.** Severe or catastrophic adverse effect (high) on organizational operations, systems, assets, individuals, or other organizations.

The security management analyzes changes to the information system to determine potential security impacts prior to change implementation. **Security impact analysis** (SIA) is conducted by internal employees with information security responsibilities (e.g., system administrators, security officers, security managers, and security engineers). Individuals conducting SIA must have the appropriate skills and technical expertise to analyze the changes (e.g., system upgrades and modifications) to information systems and the associated security ramifications.

The scope of SIA includes (1) reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls; (2) assessing risk to understand the impact of the changes and to determine if additional security controls are required; and (3) relating the amount of analysis to the impact level (i.e., a system with high impact requires more analysis).

In addition, security management analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

After the information system is changed, security management checks the security functions to verify that they are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

KEY CONCEPTS TO REMEMBER: Security

To provide reasonable security mechanisms over computer systems and networks:

- Implement access controls, firewalls, routers, sensors, hardware and software guards, and demilitarized zones to protect computer systems and networks from attacks.
- Build security now into a system, do not add it on later because it is too late, costly, and risky. Building it in requires the integration of security principles, standards, policies, procedures, controls, safeguards, and mechanisms into all phases or processes of a system development life cycle (i.e., from beginning to the end).
- Keep security as simple as possible. Complexity leads to problems in design, development, and implementation, thus making a system unusable, unstable, unmanageable, and uncontrollable and even vulnerable to threats.
- Avoid single point-of-failure situations, which are security risks due to concentration of risk in one place, system, process, or with one person. Besides placement of Web services and domain name system (DNS) servers and password synchronization problems, other causes leading to these situations include these:
  - Primary telecommunication services without backups
  - Centralized identity management
  - Central certification authority
  - Single-sign-on systems
  - Firewalls
  - Kerberos
  - Converged networks with voice and data
  - Cloud storage services and system administrators
- Fix security problems and issues correctly and timely as soon as possible.
- Practice separation of duties, whether manual or electronic.
- Require mandatory vacations for all employees.
- Practice rotation of job duties.
- Practice the principle of least privilege with secure defaults. Fail securely in a known, safe, and secure state. The efficiency and effectiveness of access control policy and its implementation depends on the system state and secure state in which the system is in at any point in time and the use of fail-safe defaults. A **secure state** is a condition in which no subject can access any object in an unauthorized manner.
- Implement system hardening techniques to make computer systems and networks more robust. To do so:
  - Remove all nonessential and unnecessary computer programs and their associated utility programs to prevent or eliminate backdoor or trapdoor attacks.
  - Implement security engineering principles (which are fully discussed in the application development section of this domain).

- Implement secure coding principles. To do so:
  - Minimize attack surface.
  - Establish secure defaults.
  - Implement the principle of least privilege.
  - Deploy the defense-in-depth principle.
  - Fail securely in a known system state.
  - Avoid security by obscurity.
  - Keep security simple.
  - Minimize programming errors that lead to software vulnerabilities.
  - Implement secure coding standards.
- Connect to a secure network (e.g., the Internet)
- Enable and configure a firewall and router.
- Install and use antivirus and antispyware software on computer systems and networks.
- Remove unnecessary software from computers and networks.
- Disable nonessential services from computers and networks (e.g., file sharing and print sharing).
- Modify unnecessary default features and options in software.
- Operate under the principle of least privilege to restrict access to computer systems and networks.
- Secure Web browsers by disabling mobile code (e.g., Active X, Java, JavaScript, VB, VBScript, Flash, and cookies).
- Apply software patches and fixes and enable future automated updates.
- Use caution and implement good security practices when opening e-mail attachments from unknown parties, (2) connecting to untrusted links, and providing sensitive information to unknown parties.
- Create strong passwords with passphrases.
- Balance the costs, risks, and benefits equation: Do not spend $10 on controls to protect an asset, information, or a risk costing $1. Costs should not exceed benefits.
- Note the trade-off that exists in security: Pay now or pay later.

(b) System Security

In this section, access controls; access control principles; access rights and permissions; access control policies; and firewalls, routers, sensors, hardware and software guards, and demilitarized zones are presented.

Access is the ability to make use of any information system's resource. Subjects (e.g., an individual, process, or device) access objects (e.g., programs, files, records, tables, processes, domains, devices, directories, and Web pages) on a computer system or network. A **subject** is an activity entity that causes information to flow among objects or changes to the system state, and an **object** is a passive entity that contains or receives information.

(i) Access Controls

Access controls are used for a number of purposes:

- To identify and authenticate users to prevent unauthorized access
- To enforce the principle of least privilege to ensure that authorized access was necessary and appropriate
- To establish sufficient boundary protection mechanisms
- To apply encryption to protect sensitive data on networks and portable devices
- To log, audit, and monitor security-relevant events

Access control is the process of granting or denying specific access requests. Access controls are of two types: physical and logical. Examples of physical access controls are listed next.

- Keys
- Visitor logs
- Physical and electronic locks
- Security guards
- Gates and guns
- Security cameras
- Smart cards and PINs
- Access codes
- Dual control
- Employee rotation of duties
- Biometrics
- Motion detectors with sensors and alarms
- Physical tokens

Examples of logical access controls are listed next.

- Passwords
- Passphrases
- PINs
- Firewalls
- Routers
- Sensors (intrusion detection systems)
- Hardware/software guards
- Demilitarized zones
- Memory/smart cards
- Hardware tokens

Preventive, detective, corrective, and recovery controls are needed to control unauthorized or illegal access to objects by subjects.

Examples of Preventive Controls

- Access control and accountability policies and procedures
- Access rules
- Account management
- Identification and authentication techniques for internal users, external users, cryptographic modules, and mobile and nonmobile devices
- Identifier management
- Authenticator management
- Session lock
- Access control enforcement by checking identity and requested access against access control lists (ACLs) and file encryption
- Information flow enforcement
- Separation of duties principle
- Least privilege principle
- Permitted actions without identification or authentication for emergencies and accessing public Web sites
- Security labels, attributes, tags, and markings
- Trust relationships in using external information systems
- Allowed and disallowed access to remote networks
- Usage restrictions for wireless access
- Restrictions in sharing information with business partners
- Separating public information from nonpublic information (e.g., personnel privacy and vendor proprietary data)
- Information system monitoring for information disclosure
- Time stamps
- Protection of audit-related information
- Audit record retention and storage capacity
- Security advisories and directives
- Information input restrictions
- Predictable failure prevention
- Security functionality verification
- Malicious code protection, including spam
- Trustworthy communications in distributed systems
- Intrusion prevention system

- Single-sign-on, reduced sign-on, and single-logout
- Web content filtering software
- Application content filters
- Security policy filters
- Blacklisting of user IDs and Internet Protocol addresses
- Security banners on computer screens

Examples of Detective Controls

- Unsuccessful login attempts
- System use notification
- Previous access logon notification to detect false logons
- Concurrent session control
- System logs
- Session audit
- Audit review, analysis, and reporting
- Security alerts
- Error handling
- Proof-of-wholeness
- Intrusion detection system

Examples of Corrective Controls

- Authenticator feedback
- Response to audit-related data processing failures
- Audit reports
- Error correction

Examples of Recovery Controls

- Fail in a known secure state
- Recover/restore to a known secure state
- Flaw remediation
- Information output handling and retention
- Audit recovery from security breaches

(ii) Access Control Principles

Access control principles include need to know, least privilege (e.g., need-to-withhold and access safety), and separation of duties, as follows.

The **need-to-know principle** is a legitimate requirement of a prospective recipient of data to know, to access, or to possess any specific and sensitive information represented by these data

to perform official tasks or services. The data custodian of the classified or sensitive unclassified information, not the prospective recipient, determines the need to know.

The **least privilege principle** states that every user and process should have the least set of privileges (i.e., restrictive set of privileges) needed to perform the task at hand. The implementation of this principle has the effect of limiting damage that can result from system errors, accidents, unauthorized use, or malicious events. This principle addresses the need for minimal interactions between privileged programs and the need to prevent improper uses of such privileges.

The least privilege principle is also related to **need-to-withhold concept**, which is the necessity to limit access to some confidential information when broad access is given to all the information. The least privilege principle is same as the need-to-know concept and is related to **access safety**, where safety includes a mechanism for preventing leakage of privileges through either constraints or confinements.

Safety is achieved from separation of duties enforced by access control policy systems.

The **separation of duties principle** is of two types: static and dynamic. In general, the purpose of separation of duty (SOD) is to ensure that failures of omission or commission with an organization are caused only by collusion among individuals, making such failures riskier and less likely. It also minimizes chances of collusion by assigning individuals of different skills or divergent interest to separated tasks; thus, SOD is enacted whenever conflict of interest may otherwise arise in assignment of tasks within an organization.

(A) Static Separation of Duty As a security mechanism, static separation of duty (SSOD) addresses two separate but related problems: static exclusivity and assurance principle.

- **Static exclusivity** is the condition for which it is considered dangerous for any user to gain authorization for conflicting sets of capabilities (e.g., a cashier and a cashier supervisor). The motivations for exclusivity relations include, but are not limited to, reducing the likelihood of fraud or preventing the loss of user objectivity.
- **Assurance principle** is the potential for collusion where the greater the number of individuals that are involved in the execution of a sensitive business function, such as purchasing an item or executing a trade, the less likely any one user will commit fraud or that any few users will collude in committing fraud.

SOD constraints may require that two roles be mutually exclusive, because no user should have the privileges of both roles. Popular SSOD policies are RBAC and RuBAC, defined later in this chapter.

(B) Dynamic Separation of Duty Separation of duties can be enforced dynamically (i.e., at access time), and the decision to grant access refers to the past access history (e.g., a cashier and an accountant are the same person who plays only one role at a time).

One type of dynamic separation of duty (DSOD) is a *two-person rule*, which states that the first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first. Another type of DSOD is a *history-based separation of duty*, which states that the same subject (role) cannot access the same object for variable number of times. Popular DSOD policies are the workflow and Chinese wall policies.

(iii) Access Rights and Permissions

Access control policies should deal with access rights in terms of file permissions, program permissions, and data permissions.

- File permissions deal with the right to create, read, edit, or delete a file on server or other places.
- Program permissions deal with the right to read, append, write, copy, change, or execute a program on an application server or other places.
- Data permissions deal with the right to view (read only), read, write, retrieve, delete, or update data in a database or file directory.

A problem with incorrect or inappropriate design of access rights and permission is authorization creep, where an authorized employee continues to maintain access rights for previously held positions within an organization. This can lead to misuse of privileges due to human error. Another problem is escalation of privileges, which can lead to exploits due to system flaws and security weaknesses.

(iv) Access Control Polices

Access control is exercised through procedures and controls to limit or detect access to critical information resources. This control can be accomplished through software, biometrics devices, or physical access to a controlled area. Access control policy is the set of rules that define the conditions under which an access may take place.

Access control *policies* are high-level requirements that specify how access is managed and who may access information under what circumstances. Policies are the set of rules that define the conditions under which an access may take place. A security policy is the statement of required protection for information objects. For instance, policies may pertain to resource usage within or across organizational units or may be based on need-to-know, need-to-withhold, competence, authority, obligation, or conflict-of-interest factors.

Access control *decisions* are usually based on access control policies, such as discretionary access control or mandatory access control. The function of access control decision is to grant or deny requests for access.

At a high level, access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. An access control list (ACL) is a familiar example of an access control mechanism. The access control mechanisms use logical, physical, and administrative controls.

Specific access control policies are listed next.

- A **discretionary access control (DAC) policy** leaves a certain amount of access control to the discretion of the object's owner or anyone else authorized to control the object's access. DAC is known as surrogate access control. DAC is generally used to limit a user's access to a file; the owner of the file controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file. A DAC policy tends to be very flexible and is widely used in the private and public sectors. This policy is often referred to as identity-based controls. It applies the need-to-know principle and uses ACLs, but not capability lists,

for implementation. DAC also uses a combination of access mechanisms for individual owners, groups, and other categories. Four basic models for DAC control exist: hierarchical, concept of ownership, laissez-faire, and centralized. DAC is a means of optionally restricting access to objects (programs and files) based on the identity of subjects (users and devices), the groups to which they belong, or both of these criteria. Access controls are discretionary in the sense that a subject with a particular access right can pass that access to any other subject. The user has control and ownership of access privileges over the items that he or she creates.

- The **nondiscretionary access control (NDAC) policy** includes all access control policies other than the DAC policy. The NDAC policy has rules that are not established at the discretion of the user. This policy establishes access controls that cannot be changed by users but only through administrative action. NDAC policies may be employed in addition to DAC policies.

WHAT ARE GENERIC ACCESS CONTROL POLICIES?

- Discretionary access control
- Mandatory access control
- Role-based access control
- Workflow access control + Chinese wall access policy
- High-latency access control

- A **mandatory access control (MAC) policy** is a means of restricting access to system resources based on the sensitivity (as represented by a security label) of the information contained in the system resource and the formal authorization (i.e., security clearance) of users to access information of such sensitivity. Users cannot change the privileges; system administrators can. MAC is often referred to as rule-based controls. It applies the marking (label) principle and uses security clearances for implementation. MAC policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user has authorized access based on classification of the information and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions.
- The **role-based access control (RBAC) policy** supports higher-level organizational policies and access control mechanisms, and RBACs are natural to the way the enterprises typically conduct their business. RBAC policy establishes coverage over all users and resources to ensure that access rights are grouped by role name and access to resources is restricted to users who have been authorized to assume the associated role.

  In the RBAC method, the role of a requester is the key determinant for access. The RBAC method better supports the implementation of *least privilege and separation of duties* but, like the identity-based access control (IBAC) method, does not scale well to. In the commercial world, RBAC is the de facto access control implementation at the enterprise level because it is what most solutions support. In fact, a role-based implementation security policy is the only logical choice for an organization that experiences a large turnover of personnel. RBAC is the privilege to use computer information in some manner based on an individual's role (i.e., teller or doctor).

- The **identity-based access control (IBAC) policy** is a mechanism based only on the identity of the subject and object. An IBAC decision grants or denies a request based on the presence of an entity on an ACL. This means that IBAC requires an authenticated identity before granting any access. IBAC and DAC are considered equivalent.
- The **rule-based access control (RuBAC) policy** is a security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. It is a mechanism for MAC policy where rules cannot be changed by users. It allows users to access systems and information based on predetermined and preconfigured rules. These controls can be combined with role-based controls such that the role of a user is one of the attributes in rule setting. The RuBAC provides for flexibility in administering security policies; however, it does not provide access assignments and constraints directly related among subjects, operations, and objects as other access control mechanisms do. RuBAC relies on security labels where labels are attached to all objects (e.g., files, directories, and devices) and sometimes to subjects (i.e., roles). In RuBAC, access to a resource is granted on the basis of an entity's authorizations rather than an entity's identity.
- A **workflow policy** separates the various activities of a given organizational processes into a set of well-defined tasks. Hence, typically, a workflow (often synonymous with a process) is specified as a set of tasks and a set of dependencies among the tasks, and the sequencing of these tasks is important. The various tasks in a workflow are usually carried out by several users in accordance with organizational rules relevant to the process represented by the workflow. The representation of a business process using a workflow involves a number of organizational rules or policies. The goal of the workflow policy is to maintain consistency between the internal data and external users' expectations of that data. The workflow management system (WFMS) is the basis for workflow policy access control system because WFMS schedules and synchronizes various tasks within the workflow.
- The **Chinese wall policy** states that once a person accesses one side of the wall, he or she cannot access the other side of the wall, thereby avoiding conflicts of interest in access. It addresses the conflict-of-interest issues related to consulting activities within banking and other financial disciplines. Like the workflow policy, the Chinese wall policy is application-specific in that it applies to a narrow set of activities that are tied to specific business transactions (e.g., giving out proprietary or insider information to outsiders). The stated objective of this policy is to prevent illicit flows of information that can result in conflicts of interest. The Chinese wall policy is often combined with MAC policy.
- In **history-based access control policies** (e.g., workflow and Chinese wall), previous access events are used as one of the decision factors for the next access authorization; the policies require sophisticated historical system-state control for tracking and maintaining of historical events.
- The **attribute-based access control (ABAC) policy** is an approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject has a set of associated attributes, such as location, time of creation, and access rights. ABAC deals with subjects, objects, targets, initiators, resources, or the environment. It uses rule sets to define the combination of attributes under which an access may take place.
- The **authority-based access control (AuBAC) policy** focuses on ABACs that can enable a RuBAC policy to be implemented based on the most current information available about a user at the time of an access attempt. In other words, AuBAC = ABAC + RuBAC.

- The **high-latency-based transaction policy** deals with provisions, prerequisites, and obligations. It can prevent identity theft, such as stealing credit/debit card numbers, Social Security numbers, driver's license numbers, bank account numbers, bank routing numbers, and other identification numbers.
- The **extensible markup language-based (XML-based) access control policy** combined with extensible access control markup language (XACML) framework provides a general-purpose language for specifying distributed access control policies. In XML terms, it defines a core schema with a namespace that can be used to express access control and authorization policies for XML objects. The XACML specification describes building blocks from which a RBAC solution is constructed. XACML has the potential to address the concerns of privilege management in terms of policy, legal, and compliance requirements. Since XACML is based on a language, it does not deal with access control processes and policy enforcements. XACML has two components: a policy enforcement point and a policy decision point. XACML uses policy combining and overriding algorithms when the policies overlap or conflict. The XML limitation, similar to RuBAC, is in the expressive power of higher-order logic, such as the expressions of historical-based constraints and domain constraints.

SUMMARY OF SPECIFIC ACCESS CONTROL POLICIES AND TECHNIQUES

- Three primary access control policies are DAC, MAC, and RBAC.
- DAC was developed originally to implement controlled sharing and to enforce the need-to-know principle. This is done with the maximum efficiency of system data and resource administration while retaining protection effectiveness.
- Both DAC and MAC policies are not well suited for private and public sectors processing unclassified but sensitive information. In these environments, security objectives often support higher-level organizational policies derived from existing policies, laws, ethics, regulations, or generally accepted practices. Such environments usually need to control individuals' actions, beyond the individuals' ability to access information, according to how that information is labeled, based on its sensitivity.
- Both DAC and MAC support lower-level organizational policies and access control mechanisms. They are unnatural to the way the enterprises typically conduct their business.
- RBAC is an improvement on DAC and MAC, but it ties users to roles and privileges toward objects.
- DAC policy implements the need-to-know principle.
- RBAC policy better supports the implementation of least privilege and separation of duties.
- DAC and IBAC policies are considered equivalent.
- MAC and RuBAC policies are considered equivalent.
- High-latency-based transaction policy deals with provisions, prerequisites, and obligations.
- ACLs, but not capability lists, are used to implement DAC, IBAC, and RuBAC policies.
- RBAC is a composite policy because it is a variant of both IBAC and RuBAC.
- RuBAC and RBAC policies can be combined so that rules can either replace or complement roles.
- Three basic access control policies are RBAC, ABAC, and IBAC. Whatever access control can be defined with IBAC or RBAC can also be defined with ABAC. In addition, the ABAC method can provide more complex access control than can be accomplished with IBAC or RBAC. However, this complexity comes with additional administrative and managerial burdens. With the ABAC method,

the policies to be supported must be known in order to assess the trade-off between capability and complexity.

- International access control policy standards do not use the U.S.-based MAC or DAC policies; instead, they use IBAC or RuBAC policies.
- The structured query language (SQL) database incorporates many aspects of RBAC and RuBAC policies.
- Nondiscretionary access control (NDAC) policies include RBAC, RuBAC, ABAC, UDAC, MAC (most mentioned NDAC), and temporal constraints, where the latter covers workflow policy and Chinese wall policy.
- The ABAC or RBAC policy is used to implement separation of domains.
- AuBAC = ABAC + RuBAC.
- RBAC and RuBAC policies are used to achieve static separations of duty.
- Workflow and Chinese wall policies are used to achieve dynamic separations of duty.
- Workflow policy is applied to organize tasks based on process rules.
- The Chinese wall policy addresses the conflict-of-interest issues arising in specific workplaces.
- Temporal constraints are related to history-based access control policies, such as workflow and Chinese wall policies.
- Note that although a person may be free to read sensitive information under the Chinese wall policy, he or she may be restricted from reading such information under a MAC policy.
- RBAC, not ABAC, implements privilege management capabilities.
- No access control policy is better or worse than any other; each has its own place and should be adopted according to its suitability for a particular set of requirements and circumstances after its strengths and weaknesses are analyzed.

Exhibit 6.4 highlights the connection between the security objectives and access control policies.

Security Objective or Goal	Access Control Policy
Confidentiality	MAC, RBAC, and Chinese wall
Integrity	Workflow
Availability	None

EXHIBIT 6.4 Linking Security Objectives to Access Control Policies

(v) Firewalls, Routers, Sensors, Hardware and Software Guards, and Demilitarized Zones

Although firewalls, routers, sensors, hardware and software guards, and demilitarized zones are classified as a part of network connectivity devices, they provide stronger system security mechanisms and hence presented here.

(A) Firewalls A firewall is a network connectivity device that mediates all traffic between two computer networks and protects one of them or some part thereof against unauthorized access. Generally, the protected network is a private, internal network. A firewall may permit messages or files to be transferred to a high-security workstation within the internal network without permitting such transfer in the opposite direction.

Many enterprise networks employ firewalls to restrict connectivity to and from the internal networks used to service more sensitive functions, such as accounting or personnel. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to its systems and resources. Inclusion of a proper firewall provides an additional layer of security. Organizations often need to use firewalls to meet security requirements from regulatory mandates.

Enclave boundary protection takes the form of firewalls and virtual private networks (VPNs). While these technologies offer perimeter and access controls, authorized internal and external (remote) users can attempt probing, misuse, and malicious activities within an enclave. Firewalls do not monitor authorized users' actions, nor do they address internal (insider) threats. Firewalls also must allow some degree of access, which may open the door for external vulnerability probing and the potential for attacks.

Configuration management activities can be extended to firewalls using a firewall rule set, which is a table of instructions that the firewall uses for determining how network packets or data packets should be routed between firewall's interfaces.

Firewall Technology Firewall technologies include packet filtering, stateful inspection, application firewalls, application-proxy gateways, dedicated proxy servers, and personal firewalls or personal firewall appliances, as discussed next.

Packet Filtering The most basic feature of a firewall is the packet filter (also known as stateless inspection firewall), operating at the network layer. A packet filter does not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that it cannot associate multiple requests within a single session to each other. Characteristics of packet filters are listed next.

- Packet filters are not concerned about the content of packets.
- Rule sets govern the access control functionality of packet filters.
- Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.

Stateless packet filters are generally vulnerable to attacks and exploits that take advantage of problems within the Transmission Control Protocol/Internet Protocol (TCP/IP) specification and protocol stack.

Stateful Inspection Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule. Unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.

Application Firewalls A newer trend in stateful inspection is the addition of a *stateful protocol analysis* capability, referred to by some vendors as *deep packet inspection.* Stateful

protocol analysis improves on standard stateful inspection by adding basic intrusion detection technology—an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations. This allows a firewall to allow or deny access based on how an application is running over the network.

Application-Proxy Gateways An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination. The proxy is meant to be transparent to the two hosts—from their perspectives, there is a direct connection. Because external hosts communicate only with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall rule set to determine whether a given instance of network traffic should be allowed to transit the firewall.

In addition to the rule set, some proxy agents have the ability to require authentication of each individual network user. This authentication can take many forms, including user ID and password, hardware or software token, source address, and biometrics.

Dedicated Proxy Servers Dedicated proxy servers differ from application-proxy gateways in that while dedicated proxy servers retain proxy control of traffic, they usually have much more limited firewalling capabilities. They have a close relationship to application-proxy gateway firewalls. Many dedicated proxy servers are application-specific, and some actually perform analysis and validation of common application protocols, such as Hypertext Transfer Protocol (HTTP). Because these servers have limited firewalling capabilities, such as simply blocking traffic based on its source or destination, typically they are deployed behind traditional firewall platforms. A main firewall could accept inbound traffic, determine which application is being targeted, and hand off traffic to the appropriate proxy server (e.g., e-mail proxy). This server would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and pass it to the firewall for outbound delivery. An example of this is an HTTP proxy deployed behind the firewall—users would need to connect to this proxy en route to connecting to external Web servers. Dedicated proxy servers generally are used to decrease firewall workload and conduct specialized filtering and logging that might be difficult to perform on the firewall itself.

Personal Firewalls or Personal Firewall Appliances Securing PCs at home or remote locations is as important as securing them at the office; many employees telecommute or work at home and use an organization's data. **Personal firewalls** usually do not offer protection to other systems or resources. They do not provide controls over network traffic that is traversing a computer network because they protect only the computer system on which they are installed.

Personal firewall appliances are similar to traditional firewalls in that they are designed to protect small networks such as those that might be found in home office. These appliances run on specialized hardware and integrate some other forms of network infrastructure components in addition to the firewall itself. These components include broadband modem wide area network (WAN) routing, local area network (LAN) routing with dynamic routing support, network hub, network switch, dynamic host configuration protocol (DHCP), simple network management protocol (SNMP) agent, and application-proxy agents.

Although both personal firewalls and personal firewall appliances address connectivity concerns associated with telecommuters or branch offices, most organizations are employing them on their intranet, practicing a layered defense strategy.

Limitations of Firewalls Firewalls can work effectively only on traffic that they can inspect. Regardless of the firewall technology chosen, a firewall that cannot understand the traffic flowing through it will not handle that traffic properly—for example, allowing traffic that should be blocked. Many network protocols use cryptography to hide the contents of the traffic (e.g., IPsec, Transport Layer Security (TLS), Secure Shell [SSH], and Secure Real-time Transport Protocol [SRTP]). Firewalls also cannot read application data that is encrypted, such as e-mail that is encrypted using the S/MIME or OpenPGP protocols or files that are manually encrypted. Another limitation of some firewalls is understanding traffic that is tunneled, even if it is not encrypted. For example, IPv6 traffic can be tunneled in IPv4 in many different ways. The content may still be unencrypted, but if the firewall does not understand the particular tunneling mechanism used, it cannot interpret the traffic.

Firewall Management Managing the firewall solution involves maintaining firewall architecture, policies, software, and other components of the solution chosen to be deployed, as described next.

- Test and apply patches to firewall devices.
- Update policy rules as new threats are identified and requirements change, such as when new applications or hosts are implemented within the network. Policy rules should also be reviewed periodically to ensure they remain in compliance with security policy.
- Monitor the performance of firewall components to ensure that potential resource issues are identified and addressed before components become overwhelmed.
- Monitor logs and alerts continuously to identify threats, successful and unsuccessful, that are made to the system.
- Perform periodic testing to verify that firewall rules are functioning as expected.
- Regularly back up the firewall policies and rule sets.
- Conduct penetration testing to assess the overall security of the network environment. This testing can be used to verify that a firewall rule set is performing as intended by generating network traffic and monitoring how it is handled by the firewall in comparison with its expected response. Employ penetration testing in addition to, rather than instead of, a conventional audit program.

(B) Routers A router is a network connectivity device that establishes a path through one or more computer networks. Routers offer a complex form of interconnectivity. The router keeps a record of node addresses and current network status. Routers are known to the end stations, as they are device dependent. LANs connect personal computers, terminals, printers, and plotters within a limited geographical area. An extended LAN is achieved through the use of bridges and routers. In other words, the capabilities of a single LAN are extended by connecting LANs at distant locations. A router operates in the network layer of the Open System Interconnection (OSI) Reference Model.

Routers convert between different data link protocols and resegment transport-level protocol data units (PDUs) as necessary to accomplish this. These PDUs are reassembled by the destination end-point transport protocol entity. There are several routing protocols in common use.

Routers must have more detailed knowledge than bridges about the protocols that are used to carry messages through the internetwork. When routers are used to connect fiber distributed data interface (FDDI) to other networks, it is important to be certain that the routers support the needed network level protocols.

WHAT IS AN INFORMATION TECHNOLOGY PERIMETER SECURITY DEFENSE?

An information technology perimeter security defense is a method that integrates security of all layers of the architecture, including router, switch, network, operating system, file system, database, and applications layers.

Router Accounts and Passwords Restricting access to all routers is critical in safeguarding the network. In order to control and authorize access, an authentication server that provides extended user authentication and authority levels should be implemented.

For router accounts and passwords, the router administrator will ensure:

- An authentication server is used to gain administrative access to all routers.
- When an authentication server is used for administrative access to the router, only one account is defined locally on the router for use in an emergency (i.e., authentication server or connection to the server is down).
- Each user has his or her own account to access the router with username and password.
- All user accounts are assigned the lowest privilege level that allows them to perform their duties.
- Accounts that are no longer required should be removed immediately from the authentication server or router.
- A password is required to gain access to the router's diagnostic port (management port used for troubleshooting).
- The enable secret password must not not match any other username and passwords, enable password, or any other enable secret password.
- Passwords are not viewable when displaying the router configuration.

Routing Table Integrity A rogue router could send a fictitious routing table to convince a site's premise router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information of the site's network or merely used to disrupt the network's ability to communicate effectively with other networks.

Router Packet Filtering and Logging ACLs are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of routers makes use of ACLs for restricting access to services on the router itself as well as for filtering passing through the router.

Router Configuration Management Configuration management activities can be extended to routers using rule sets, similar to firewalls. The rule set can be a file that the router examines from top to bottom when making routing decisions, using routing tables.

(C) Sensors Sensors are intrusion detection systems (IDSs) and are composed of monitors and scanners, and they fill the gap left by firewalls. *Monitors* are of two types: network monitors and host monitors. Both types of monitors perform intrusion detection and malicious code detection. *Scanners* are of two types: network scanners and host scanners. Network scanners provide vulnerability scanning and war dialing. Host scanners provide vulnerability scanning and file integrity checking. Both monitors and sensors must have detect and respond capabilities.

IDSs are hardware and software products that gather and analyze information from various areas within a computer or network to identify possible security breaches. These breaches include intrusions from outside the organization and misuse from within the organization. An IDS is a system to detect, report, and provide limited response to an activity that may be harmful to an information system. Some IDSs can even prevent the intrusion activities. Tools to complement the IDSs include antimalware products (i.e., antivirus software, antispyware software), firewalls, routers, honeypots, honeynets, padded cell systems, and canaries.

(D) Hardware and Software Guards Hardware and/or software guards enable users to exchange data between private and public networks, which is normally prohibited because of information confidentiality. A combination of hardware and/or software guards is used to allow secure LAN connectivity between enclave boundaries operating at different security classification levels (i.e., one private and the other public).

A guard is a device used to defend the network boundary by employing these functions and properties:

- Guards typically are subjected to high degree of assurance during development.
- They support limited services.
- Services are at the application level only.
- Guards may support application data filtering reviews.
- Guards may support sanitization of data.
- Typically they are used to connect networks with differing levels of trust (i.e., provide regrading of data).

Guard technology can bridge across security boundaries by providing some of the interconnectivity required between systems operating at different security levels. Several types of guards exist. These protection approaches employ various processing, filtering and data-blocking techniques in an attempt to provide data sanitization (e.g., downgrade) or separation between networks. Some approaches involve human review of the data flow and support data flow in one or both directions. Information flowing from public to private networks is considered an upgrade. This type of transfer may not require a review cycle but should always require a verification of the integrity of the information originating from the public source system and network. Guards can be used to counteract attacks made on the enclave.

A guard is designed to provide a secure information path for sharing data between multiple system networks operating at different security levels. The guard system is composed of a server, workstations, malicious code detection, a firewall, and/or filtering routers, all configured to allow transfer of information among communities of users operating at different security levels.

Most guard implementations use a dual network approach, which physically separates the private and public sides from each other. Guards are application specific; therefore, all information will enter and exit by first passing through the Application Layer, Layer 7 of the OSI model. In addition, most guard processes are high-assurance platforms that host some form of trusted operating system and trusted networking software.

Enclave boundaries need protection from the establishment of unauthorized network connections. The focus is on attacks into an enclave by malicious e-mail transfer, file transfer, or message transfer. Guards can be implemented to provide a high level of assurance for networks by preventing certain types of malicious messages from entering the enclave.

(E) Demilitarized Zones A demilitarized zone (DMZ) is an interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.

A DMZ is a separate network subnet designed to expose specific services to a larger, untrusted network. The subnets are used in large corporations or organizations to safely expose functions to the Internet, such as Web or database applications. DMZs also are used internal to networks to facilitate secure data transfer from a high-security network zone to a zone with lower security. A DMZ uses explicit access control and contains computer hosts that provide network services to both low-security and high-security network zones. DMZ networks are usually implemented with a firewall or other traffic routing network device. They can be split into several sub-DMZ networks with specific functional groupings for the computers, such as Web servers, timeservers, or file transfer protocol (FTP) repositories. Having multiple DMZs protects the information resources from attacks using virtual LAN hopping and trust exploitation, thus providing another layer to the defense-in-depth strategy.

A possible architecture is to use firewalls with the ability to establish a DMZ between two networks. The use of a DMZ-capable firewall allows the creation of an intermediate network. Creating a DMZ requires that the firewall offer three or more interfaces rather than the typical public and private interfaces. If a patch management server, a Web server, an authentication server, a system log (syslog) server, a remote access server, a DNS server, an antivirus server, or a VPN server is to be used for a network, it should be located directly on the DMZ. Limitations of DMZ include that it **c**annot work by itself and needs to work with a firewall or router.

(c) Information Protection

In this section, topics such data and information, threats and vulnerabilities, threat events, threat sources, information protection methods, privacy management, and compliance with privacy laws and information protection laws and regulations are discussed.

(i) Data and Information

Data is a collection of facts and figures, and it is usually expressed as numbers. Information is data that is:

- Computed using mathematical equations and formulas.
- Aggregated or summarized in a designated way.

- Combined with several data items in different ways.
- Compared and contrasted in some manner.
- Analyzed and reported in some manner.
- Arranged or sorted either in ascending or descending order.
- Otherwise manipulated or massaged in different ways.

In other words, data is raw data, and information is processed data. Data by itself is meaningful to some whereas information is meaningful to many, because information is derived from data. Most people use the terms "data" and "information" interchangeably and loosely.

A simple example will suffice here: Raw data is when an employee's number of hours worked in a week is 40 hours and the hourly wage rate is $15 per hour. Information is when this employee's payroll check shows the weekly gross earned amount of $600 and weekly gross earned amount for 10 employees is $6,000.

Information, data, software, copyrights, trade secrets,, trademarks, and patents are a big part of an organization's intangible (vital) assets, similar to tangible (physical) assets, such as computers, terminals, workstations, scanners, plotters, printers, fax machines, network-related equipment (e.g., cables, wires, and devices), mobile devices (e.g., regular phones, smartphones, personal digital assistants [PDAs], digital pads and tablets), and portable storage devices (e.g., disks, flash drives, thumb drives, pen drives, tapes, and paper). These intangible assets, especially data and information, are vital assets, so they must be protected at all times because an organization's management depends on them in day-to-day, short-term, and long-term decision-making processes. Note that tangible assets either contain or store these intangible assets.

Possible risks for data and information include destruction, loss, damage, or stealing credit and debit card information and Social Security numbers, and disclosure to unauthorized parties, which leads to privacy issues and legal disputes.

Specifically, these vital assets are easily and constantly exposed to greater risks from insiders (current employees, disgruntled, employees, and previous employees) and outsiders (e.g., attackers, hackers, adversaries, suppliers, vendors, customers, contractors, and business partners) for their personal and financial gain, including intelligence-gathering purpose for competitive reasons.

Data and information are spread out everywhere in an organization and in all organizations. Because of this, most people want these assets since they have intrinsic and extrinsic value. These vital assets, such as data and information, are the major targets of insiders and outsiders alike. For example, insiders (managers and executives) want them for decision making and to run business operations. Outsiders (e.g., attackers, adversaries, competitors, consultants, contractors, suppliers, and vendors) want them for personal gain, financial benefit, competitive advantage, grudge, revenge, and even fun. Therefore, data and information must be protected at all times and with whatever means necessary.

If data and information are so vital, how well are organizations protecting them? The answer is not so well because threat sources are constantly changing, vulnerabilities are increasing rapidly, security controls are not adequate or appropriate, and attackers are getting more sophisticated in their attack methods.

(ii) Threats and Vulnerabilities

A **threat** is any circumstance or event with a potential to adversely impact an organization's operations (e.g., mission, functions, image or reputation), assets, information, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or even denial of service. Also, a potential for a threat source can exploit a particular system's vulnerability. These threats, whether cyber or not and whether local or global, have far-reaching negative effects with increasing speed. The presence of a threat event does not mean that it will necessarily cause actual harm or loss. To become a risk, a threat must take advantage of vulnerabilities in system security features and controls.

A **vulnerability** is a fault, weakness, bug, or a security hole in a system's functions and operations, security procedures, and design and implementation of internal controls that could be exploited or triggered by a threat source.

A relationship exists among vulnerabilities, threats, risks, and controls, as follows:

Vulnerabilities→Threats→Risks→Controls

Lack of adequate and/or inappropriate controls often increases the vulnerabilities in a system. Therefore, one needs to focus on vulnerabilities first, threats next. Note that controls reduce risks.

(iii) Threat Events

Many threat events are looming around over in all organizations, including these, to name a few:

- Business corporations
- Governmental agencies, including defense
- Industrial control systems
- Electric power grid systems
- Railroad computer systems
- Gas utility systems
- Water purification and pumping station computer systems
- Oil refinery computer systems
- Personal computer systems.

(iv) Threat Sources

Many threat sources exist. A number of such attack sources are listed next.

- Malware and malicious code (e.g., viruses, worms, logic bombs, time bombs, and Trojan horses)
- Mobile code on mobile devices (e.g., mobile botnets, mobile applications, exploitation of mobile commerce, exploitation of social media networks, and social engineering)
- Web browser–based attacks (e.g., browser session hijacking, applets, flash, Active X, Java, plug-ins, cookies, JavaScript, and VBScript)
- Eavesdropping (e.g., packet snarfing)
- Masquerading (i.e., impersonating, spoofing, and mimicking)

(v) Information Protection Methods

Several protection methods are available to protect valuable data and information. A number of these are listed next.

- **Deploy a defense-in-depth strategy.** Securing data/information and computer systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of IT. This is due to the highly interactive nature of the various systems and networks and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured.

  By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of IT assets for the purpose of achieving its objectives. The concept of layered protections is called security in depth.

  The defense-in-depth strategy recommends two information assurance principles: defense in multiple places and layered defenses.

  - **Defense in multiple places.** Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. As a minimum, these defensive focus areas should include defending:
    - The networks and infrastructure by (a) protecting the local and wide area communications networks from denial-of-service (DOS) attacks and (b) providing confidentiality and integrity protection for data transmitted over these networks by using encryption and traffic flow security measures to resist passive monitoring.
    - The enclave (envelope) boundaries by deploying firewalls and intrusion detection mechanisms to resist active network attacks.
    - The computing environment by providing access controls on hosts and servers to resist insider, close-in, and distribution attacks.
  - **Layered defenses.** In no time, adversaries find an exploitable vulnerability. An effective countermeasure is to deploy multiple defense mechanisms between the adversary and the target. Each of these mechanisms must present unique obstacles to the adversary. Further, each mechanism should include both protection and detection measures. These help to increase risk of detection for the adversary while reducing chances of success or by making successful penetrations unaffordable. Deploying nested firewalls, each coupled with intrusion detection, at outer and inner network boundaries is an example of a layered defense. The inner firewalls may support more granular access control and data filtering.
- **Deploy a defense-in-breadth strategy.** This strategy includes a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). This strategy deals with scope-of-protection coverage of a system. It is also called supply chain protection control. It supports agile defense strategy and is the same concept as security in depth.

- **Deploy a defense-in-technology strategy.** This strategy deals with a diversity of information technologies used in the implementation of a system. Complex technologies can create complex security problems.
- **Deploy a defense-in-time strategy.** This strategy deals with applying controls at the right time and at the right geographic location. It considers global systems operating at different time zones.

WHICH SECURITY DEFENSIVE STRATEGY DEALS WITH WHAT?

- The defense-in-depth strategy deals with controls placed at multiple levels and at multiple places in a given system.
- The defense-in-breadth strategy deals with scope-of-protection coverage of a system.
- The defense-in-technology strategy deals with a diversity of information technologies used in the implementation of a system.
- The defense-in-time strategy deals with applying controls at the right time and at the right geographic location.

- **Deploy agile defenses with the concept of information system resilience. Agile defense** assumes that a small percentage of threats from cyberattacks will be successful by compromising information systems through the supply chain by defeating the initial security controls implemented by organizations or by exploiting previously unidentified vulnerabilities for which protections are not in place. In this scenario, adversaries are operating inside the defensive parameters established by organizations and may have substantial or complete control of systems.

  Information system resilience is the ability to quickly adapt and recover from any known or unknown changes to the system environment through holistic implementation of risk management, contingency mechanisms, and continuity planning.

  Agile defense employs the concept of information system resilience, that is, the ability of systems to operate while under attack, even in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. The concept of system resilience can be applied not only to cyberattacks but also to environmental disruptions and human errors of omission or commission. The agile defense and system resilience concepts should be combined with defense-in-depth and defense-in-breadth strategies to provide a stronger protection against attacks.
- **Install several lines of defenses.** The lines of defenses are security mechanisms for limiting and controlling access to and use of computer system resources. They exercise a directing or restraining influence over the behavior of individuals and the content of computer systems. They can be grouped into four categories—first, second, last, and multiple—depending on their action priorities. A first line of defense is always preferred over the second or the last. If the first line of defense is not available for any reason, the second line of defense should work. These lines of defenses form a core part of defense-in-depth strategy or security-in-depth strategy. If the second line of defense is not available or does not work, then the last line of defense must work. The term "multiple defenses" here denotes more than one control, device, policy, layer, factor, mode, or level acting in concert to provide greater synergy, strength, and security to a system.

Multi-user, multiplatform, remote access, resource-sharing, and data-sharing computer systems require different and stronger controls than single-user, single-platform, and local access systems. For a multi-user environment, a minimum security requirement should be provided as a reasonable first line of defense against an unauthorized user's attempt to gain access to the system or against an authorized user's inadvertent attempt to gain access to information for which he or she has not been granted access.

Examples follow for each of these four lines of defenses.

First Line of Defense

- Network infrastructure between the Internet and a public Web server
- Policies and procedures against people's bad behavior
- Internal controls, especially preventive controls, against bad business practices
- Passwords and user identification codes against unauthorized access and use of computer system resources
- Firewalls and software/hardware guards against network compromises (e.g., attacks by outsiders)
- Border routers
- Separation of duties against errors, omissions, irregularities (e.g., fraud and theft), and system compromises
- Identification and authentication techniques against unauthorized access (e.g., impostors and impersonators)
- Training, awareness, and education against weak technical and procedural safeguards
- Physical security controls (e.g., keys and locks, and access control systems) against unauthorized entry and exit and to prevent access to computer hardware and servers
- Network monitoring against spoofing attacks
- Quality assurance against poor quality, inconsistency, or poor integrity
- Vigilant and diligent system/security administrators against system tampering, fraud, abuse, and intrusions
- Fault tolerant (e.g., disk-mirroring and Redundant Arrays of Independent Disks [RAID] technology) and redundancy (duplicate equipment) techniques against data loss and Denial of Service (DoS) attacks
- Security containers to place objects
- Entrapment techniques against attacks by outsiders using fake data and systems (decoys and honeypot systems)
- Program change controls against unauthorized program changes
- Dial-back technique against unauthorized access
- Limited unsuccessful attempts prior to login connectivity
- Perimeter barriers, such as gates, fences, and human security guards, against property damage, intrusion, or unauthorized entry and exit
- Integrity verification software against poor-quality data

- System isolation techniques against virus and other attacks
- Sprinkler systems, water detectors, waterproof covers, and temperature regulators
- Minimum security requirements against an unauthorized user's attempt to gain access to the system or against an authorized user's inadvertent attempts to gain access to information for which he or she has not been granted access in a multi-user and multiplatform environment
- Split knowledge procedures against compromise of system integrity and system components
- Employee security and employment policies, procedures, and practices (screening and clearance procedures and education, experience, and background verification procedures before hiring; access agreements and employment contracts after hiring; return of company property [e.g., keys, ID cards, and building passes]) and disconnection of system access after termination of employment
- Third-party security provider policies, procedures, and practices defining roles, responsibilities, and sanctions for contractors, consultants, outsourcers, service bureaus, and other organizations providing IT products and services
- Network-based computing environment consisting of LANs, Integrated Services Digital Networks (ISDNs), and WANs

Second Line of Defense

- Audit trails and logs against unauthorized actions (e.g., additions, changes, and deletions)
- Monitoring of systems and employees against unauthorized actions (e.g., monitoring employees through keyboard strokes)
- Attack-detection software against harmful attacks
- Penetration testing (e.g., blue team or red team testing) against circumventing the security features of a computer system
- Exterior protection, such as walls and ceilings, against unauthorized entry
- Automated alarms and sensors to detect abnormal events

Last Line of Defense

- Software testing against design and programming defects
- Property insurance against disasters (natural and man-made)
- Insurance bonding coverage against dishonest employees and contractors
- Backup files to recover from lost data
- Host-based computing environment consisting of workstations and servers
- Configuration management practices against improper release of a system prior to its distribution and use
- Quality control checks and integrity control checks and inspection tests against poor quality
- Contingency planning against unforeseen events and conditions

- Security assessments to determine the overall effectiveness of the security controls in an information system.
- Employee vigilance against anything that has escaped the first and/or second line of defense mechanisms

Multiple Lines of Defense

- Employ multilayered controls, where controls are layered, as in defense-in-depth and defense-in-breadth strategies.
- Use multifactor authentication systems, where two factors or three factors are used to authenticate a person, system, process, or device.
- Employ multilevel testing, where several types of testing are conducted for cryptographic modules.
- Use multilayer system security services, where operating system security service layers are working together with distributed system security service layers and user application system security service layers. Each layer can depend on capabilities supported by lower layers.
- Use multilevel security policies, where a subject is permitted to access an object only if the subject's security level is higher than or equal to the object's security classification level.
- Employ a multilevel security mode, where the mode handles multiple information classification levels at a number of different security levels simultaneously
- Use multilayered switches, where they can look deeper within a network packet and make informed decisions based on the data found there to facilitate better routing and traffic management tasks.
- Use multihomed firewalls, which can create several independent DMZs—one interfacing the Internet (public network), one interfacing the DMZ segments, and another one interfacing the internal company network. These firewalls work with more than one network interface card (NIC).

- Implement traditional backup methods to protect data files, computer programs, and computer systems with full backups, incremental backups, differential backups, and hybrid backups (e.g., a full backup on the weekend and a differential backup each evening). These backup methods are good for disks and tapes. Remember that "no backup means no recovery" from disasters and damages to organization's assets.
- Implement a zero-day backup method, which is similar to traditional or full backup, which archives all selected files and marks each as having been backed up. This method is the fastest restore operation because it contains the most recent files. A disadvantage is that it takes the longest time to perform the backup.
- Deploy advanced backup methods on large storage media using disk arrays (e.g., redundant array of independent disk, RAID technology), which are a cluster of disks used to backup data onto multiple disk drives at the same time, to provide data protection, data availability, and data reliability.
- Defend attack-in-depth strategies and zero-day attacks. Malicious code attackers use an **attack-in-depth strategy** to carry out their goals. Single-point solutions will not stop all of their attacks because a single countermeasure cannot be depended on to mitigate all security issues. In addition, a single-point solution can become a single point of failure (or

compromise) that can provide extended access due to preexisting trust established among interconnected resources.

The attack-in-depth strategy can create advanced persistent threats where an adversary with sophisticated expertise and significant resources can create opportunities to achieve its objectives by using multiple attack vectors, such as cyber, physical, logical, and deception. Mitigate advanced persistent threats with agile defenses combined with boundary protection controls. Agile defense employs the concept of information system resilience.

Multiple countermeasures against attack-in-depth strategy include agile defenses, boundary protection controls (e.g., firewalls, routers, and software/hardware guards), defense-in-depth strategy, and defense-in-breadth strategy because they can disseminate risks over an aggregate of security mitigation techniques.

- Protect Web browsers from attacks by: (1) disabling mobile code on Web sites that you are not familiar with or do not trust; (2) disabling options to always set cookies; and (3) setting the security levels for trusted Web sites (i.e., those that you most often visit and trust) to the second highest level. Note that at the highest security level, some Web sites may not function properly.
- Implement strong password methods such passphrases, encrypted passwords, and dynamic passwords with challenge-response protocols to protect password-based attacks, including brute-force password attacks.

Password management may seem simple, but it is not simple when doing business on the Internet. One should not think that some passwords are less important than others because all passwords are important to hackers. Some hackers can piece together password-related information stored online and shared on social media networks. Another risk is that some commercial Web sites give customers the ability to store billing and shipping addresses along with their credit/debit card information. Bank account numbers, Social Security numbers, User IDs, and passwords. This could lead to **identity theft**, which involves stealing personal information (mostly financial) and using it illegally. It is a form of phishing attack.

Some guidelines to protect against identity theft are listed next.

- **Never provide your personal information in response to an unsolicited request**, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
- **If you believe the contact may be legitimate, contact the financial institution yourself.** You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.
- **Never provide your password over the phone or in response to an unsolicited Internet request or phone request.** A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.
- **Review your bank account statements regularly to ensure all charges are correct.** If your account statement is late in arriving, call your financial institution to find out why.

If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.

Three common mistakes many users make with passwords and remedies for them are listed next.

Mistake 1: Using a weak password, such as common phrases, dictionary terms, name, and birthday.

Remedy 1: Use a passphrase that is long, is not a common phrase, includes numbers, lowercase and uppercase letters, and special characters (e.g., punctuation, a dollar sign, or pound sign).

Mistake 2: Using the same password for every account.

Remedy 2: Use a different password for each Web site with password manager software, which is an encrypted database.

Mistake 3: Exposing passwords to others, such as logging in from a public computer, keeping a note with passwords written on it where it can be found, or sharing passwords with others.

Remedy 3: Avoid the use of public computers and public access networks, if possible. If there is a need to use them, do not send or receive private, sensitive, or confidential information, and change the password afterward. Store passwords in an encrypted file or password manager and avoid sharing passwords.

- Install software patches, updates, hot fixes, and service packs for operating system software and applications in a timely manner to close security holes and to avoid potential vulnerabilities. The goal is to implement a robust software patch management process in order to reduce vulnerabilities in an information system. As patches greatly impact the secure configuration of an information system, the patch management process should be integrated into configuration management at a number of points, as follows.
  - Perform security impact analysis of patches.
  - Test and approve patches as part of the configuration change control process.
  - Update baseline configurations to include current patch level.
  - Assess patches to ensure they were implemented properly.
  - Monitor systems/components for current patch status.
- Understand zero-day exploits and zero-day incidents (attacks). Zero-day exploits (i.e., actual code that can use a security vulnerability to carry out an attack) are used or shared by attackers before the software vendor fixes those exploits. A **zero-day attack** or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others, undisclosed to the software vendor, or for which no security fix is available. This is a timing game sophisticated attackers play on user organizations. Most organizations are helpless in the face of these attacks.
- Protect data on storage media with sanitization methods, such as overwriting (i.e., clearing), degaussing (i.e., purging), and physical destruction (i.e., disintegration, pulverization, melting, incineration, shredding, sanding, and acid solutions). Overwriting, not erasing, is an effective method for clearing data from magnetic media because the deleted data cannot be retrieved later on. The same thing cannot be said for the erasing. Note that destruction is a strong form of sanitization; disposal in a waste container is a weak form

of sanitization. The goal is to ensure that there is no residual data on the storage media because attackers can target it for personal gain. Remember that residual data is residual risk for the user organization.

- Sanitize computer memory, both volatile memory and nonvolatile memory, to prevent memory leakage to attackers. The contents of volatile memory found in random access memory (RAM) chips can be sanitized by removing the electrical power from the chip; the chip requires power to maintain its content. The contents of nonvolatile memory as found in programmable read-only memory (PROM) flash memory is permanent until reprogrammed; it can be sanitized using ultraviolet light, overwriting, and physical destruction.
- Protect data at rest with cryptographic mechanisms, which are discussed in the encryption section of this domain. The scope of data at rest, data in storage, or data on a hard drive includes protecting the confidentiality, integrity, and availability of data residing on servers, workstations, computers, storage/disk arrays (e.g., RAID), network-attached storage appliances, disk drives, tape drives, and removable media, such as flash drives, thumb drives, and pen drives.
- Protect data in transit with cryptographic mechanisms, which are discussed in the encryption of this domain. The scope of data in transit, data in flight, or data on the wire includes protecting the confidentiality, integrity, and availability of data as they are transferred across the storage network, the LAN, and the WAN.
- Protect from dumpster-diving activities (i.e., physical scavenging) by shredding sensitive or confidential documents instead of disposing them in recycling bins (which are high risk).
- Protect from industrial espionage activities (i.e., electronic scavenging) by sanitizing (e.g., degaussing and overwriting) the electronic storage media.
- Protect from hardware-based and software-based key logger attacks, which are spyware attacks. Hardware devices usually slip inline between the keyboard cable and computer; they are difficult to install because doing so requires physical access to the cable and computer. Software key loggers capture keyboard events and record the keystroke data before it is sent to the intended application for processing. As a remedy, install antispyware software.
- Protect configuration data by creating a "gold disk" (master disk) that contains a baseline configuration data about an operating system so that the system's software, ports, system services, and login credentials are run in a safe and efficient manner, using the gold disk. This master disk contains all the necessary information about configuration in one place, instead of several places. Ensure that the gold disk does not contain guest accounts and unnecessary user accounts and that it contains only the least amount of privileges. Because of this approach, the gold disk increases the security posture and lowers the attack surface. Even with a gold disk, however, misconfiguration is possible. This security risk leading to a security breach should be managed well. **Misconfiguration** means that initial configuration settings are established incorrectly and inappropriately or implemented ineffectively and that changes to configuration data are made incorrectly. Misconfiguration leads to vulnerability. Configuration management is fully discussed in the application development section of this domain.
- Implement fault-tolerance mechanisms, such as fail-stop processors and redundancy mechanisms with fault detection, error recovery, and failure recovery abilities. Refer to the business continuity section of this domain for full details.
- Control superusers, special privileged users, privileged programs, guest accounts, and temporary accounts. A **superuser** is a user who is authorized to modify and control IT

processes, devices, networks, and files. Special privileged users are given permissions to access files, programs, and data beyond normal users, thus creating a security risk. Privileged programs are those programs that, if unchecked, could cause damage to computer files (e.g., some utility programs).

- Install antivirus software to control viruses and other forms of malware, and keep it up-to-date with current signatures.
- Implement stackguarding technology to prevent buffer overflow exploits, which, in turn, lead to worm attacks.
- Install spam-filtering software, Web content filtering software, Bayesian spam filters, whitelists, and blacklists to control spamming attacks.
- Implement antispoofing methods to prevent the unauthorized use of legitimate identification and authentication data.
- Install antispyware software to detect both malware and nonmalware forms of spyware attacks, such as browser session hijacking, cookies, Web bugs, and bots.
- Install antijam methods to control jamming attempts. The antijam methods ensure that transmitted information can be received despite deliberate jamming attempts. Jamming is an attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unstable.
- Install Web content filtering software to control Web bugs. A Web bug is a tiny image of a malicious code, invisible to a user, placed on Web pages, Web sites, or Web browsers to enable third parties to track use of Web servers and collect information about the user, including IP address, host computer name, browser type and version, operating system name and version, and cookies. Web content filtering software is a program that prevents access to undesirable Web sites, typically by comparing a requested Web site address to a list of known bad Web sites. In general, content filtering is the process of monitoring communications, such as e-mails and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.
- Implement the Kerberos authentication protocol to provide authentication and authorization of users and systems on the network. This protocol uses symmetric cryptography.
- Implement digital signatures, digitized signatures, electronic signatures, and digital certificates to provide a strong form of authentication. See the encryption section of this domain for more details.
- Keep your browser settings and e-mail configurations current and accurate to control Internet-based attacks.
- Protect from social engineering and pretexting attacks, which are nontechnical methods, through system user training and education, by implementing good computing practices, by advising system users and administrators to be more vigilant, and by using electronic tokens with dynamic authenticators.

(vi) Privacy Management

Privacy deals with balancing individual rights in a society. Two definitions exist: (1) the individual right to determine the degree to which one is willing to share information about oneself that may be compromised by unauthorized exchange of such information among other individuals or organizations and (2) the individual and organizational rights to control the collection, storage, and dissemination of information.

Privacy is the right of an individual to limit access to information regarding that individual. Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. **Confidentiality** refers to disclosure of information only to authorized individuals and entities.

Privacy means that the rights of the accused (suspect) cannot be violated during an investigation. The accused can use protective orders if his or her privacy rights are ignored or handled improperly. If accused persons can prove that evidence brought against them would do more harm to them than good, the courts will favor the accused in suppressing such evidence from being presented.

With respect to information systems, privacy deals with the collection and use or misuse of personal data. The issue of privacy deals with the right to be left alone or to be withdrawn from public view. Privacy at work creates conflict between employers wanting to monitor employees' work activities and employees who resent such monitoring. For example, computer workstation software can track employee keystrokes made at the PC keyboard. Another privacy issue is e-mail at work. Courts have ruled that a privileged communication does not lose its privileged character if it is communicated or transmitted electronically. E-mail is a controversial topic; many state and federal laws have been passed in this area.

Another area of privacy concern is the Internet, where a Web site collects personal information (e.g., cookies) when potential or actual customers are buying or selling goods or services or simply inquiring. Individuals should protect their personal information by finding out what data is stored and how it is used, by not using a work e-mail system to send personal e-mails, and by not sharing personal information without written consent.

(A) Privacy Risks Privacy risk originates from divulging or releasing personal financial information, personal medical information, trade secret formulas, and other sensitive information (e.g., salaries) about an individual to unauthorized parties.

Best practices to reduce privacy risks are listed next.

- Install a privacy officer or its equivalent.
- Develop and communicate privacy policies that contain consequences for not complying with them.
- Understand privacy laws and regulations.
- Implement policies and procedures for controlling and releasing personal information to third parties.
- Provide employee orientation classes by the human resources department at the time of hiring.
- Conduct privacy audits, special management reviews, and privacy self-assessment reviews periodically and proactively to reduce privacy risks.

(B) Privacy Impact Assessments Organizations should conduct privacy impact assessments (PIAs), which are processes for examining the risks and ramifications of collecting, maintaining, and disseminating information in identifiable form in an electronic information system. The

assessments also include the means for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form.

PIAs should be performed and updated when a system change creates new privacy risks. Examples of system changes are listed next.

- When converting a paper-based records into electronic-based records
- When anonymous information changes to nonanonymous state (i.e., information from nonidentifiable form to an identifiable form)
- When significant system changes occur in technology and databases
- When user-authenticating mechanisms (e.g., passwords, digital certificates, and biometrics) are new to an automated system

PIAs must address the next issues.

- What information is to be collected (e.g., to determine eligibility)
- Why the information is being collected (e.g., nature and source)
- The intended use of the information (e.g., to verify data)
- With whom the information will be shared (e.g., internal and external)
- What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared (e.g., choice of declining voluntary information or consenting to particular use of that information)
- How the information will be secured (e.g., administrative and technical controls)
- Whether a system of records is being created (e.g., audit trails)

(vii) Compliance with Privacy Laws and Information Protection Laws and Regulations

Many laws and regulations apply to privacy of information and information protection both inside and outside the United States. For example:

- The U.S. Privacy Act of 1988 requires protection of information related to individuals maintained in the U.S. federal information systems and grants individuals access to the information concerning them. This act is applicable to both public sector and private sector organizations. This act defines 11 privacy principles, as follows:
  1. Manner and purpose of collection of personal information
  2. Solicitation of personal information from individual concerned
  3. Solicitation of personal information generally
  4. Storage and security of personal information
  5. Information relating to records kept by the record keeper
  6. Access to records containing personal information
  7. Alteration of records containing personal information
  8. Record keeper to check accuracy and completeness of personal information before use
  9. Personal information to be used only for relevant purposes

10. Limits on use of personal information
11. Limits on disclosure of personal information

- The U.S. Computer Security Act of 1987 requires U.S. federal government agencies to identify sensitive systems, conduct computer security training, develop computer security plans, and protect computer-related assets.
- The U.S. Fair Credit Reporting Act protects consumer report information.
- The U.S. Gramm-Leach-Bliley Financial Modernization Act of 1999 protects nonpublic personal information collected and used by financial institutions.
- The U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996 protects health information collected by health plans, health care clearinghouses, and health care providers.
- The U.S. Federal Trade Commission is responsible for ensuring consumer protection and market competition.
- The European Union's (EU's) directive on data protection is concerned about the transfer of data over countries. See www.eurunion.org.) This directive mandates that companies engaging in transborder data flows maintain an "adequate level" of privacy protection for such data. The EU also issued an international safe harbor privacy principle dealing with notices, choices, transfers, security, data integrity, access, and enforcement among its member countries or nations. Other EU directives deal with these topics:
  - Information security
  - Antispam laws
  - Attacks against information systems
  - Legal aspects of electronic commerce
  - Access to electronic communications
  - Protection of personal data in databases
  - Protecting intellectual property
  - Safer Internet Plus Programme (i.e., no illegal or harmful content)
  - Unsafe commercial practices, such as misleading and aggressive practices, including pyramid schemes and bait advertising.
- The Organisation for Economic Co-operation and Development (OECD; www.oecd.org) issued guidelines to protect privacy and personal data and on obviating unnecessary restrictions to transborder data flows, both online and offline. It also issued guidelines to control:
  - Spam attacks
  - Cross-border cooperation in protecting privacy
  - Cryptography
  - Electronic authentication
  - Identity management
  - Protecting consumers from fraudulent and deceptive practices across borders
  - Security of information systems and networks

(d) Identification and Authentication

Identification purpose, application authentication techniques for system users, application authentication techniques for devices, identity management and privilege management, and integrating identification and authentication methods are discussed in this section.

(i) Identification Purpose

Identification refers to establishing the identity of a user, process, or device prior to authentication. It is the means by which a user provides a claimed identity to the system. **Authentication** is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to system resources. It is the means of establishing the validity of this claim. **Authorization** is the process of defining and maintaining the allowed actions. **Accountability** is making individuals responsible for their actions and inactions equally, and it supports the identification, authentication, and audit requirements, nonrepudiation, deterrence, fault isolation, intrusion prevention and detection, and after-action recovery and legal action. Accountability should be reflected in audit trails. Access rules support accountability.

Identification and authentication (I&A) establishes the basis for accountability, and the combination of all three enables the enforcement of identity-based access control. The correct sequence of actions taking place in an access control mechanism is as follows:

Identification→Authentication→Authorization→Accountability

Note that identification comes before authentication, authorization comes after authentication, and accountability comes after authorization.

The user's identity can be authenticated using the following basic I&A mechanisms:

- Knowledge-based I&A techniques (e.g., what you know, using password, user ID, username, or PIN)
- Token-based I&A techniques (e.g., what you have, using memory card, smart card, personal identification verification [PIV] card, hardware token, noncryptographic key, and digital certificate)
- Physical location–based I&A techniques (e.g., where you are, using global positioning system [GPS] and wireless sensor network)
- Biometrics-based I&A techniques (e.g., what you are, using fingerprints for, iris recognition for, and what you are using the dynamic biometrics, such as handwriting and voice recognition, for)

Biometrics is the science and technology of measuring and statistically analyzing biological data. In IT, the term usually refers to technologies for measuring and analyzing human body characteristics, such as voice and facial pattern recognitions, eye retina scans, and hand measurements (e.g., fingerprints, handwriting, hand geometry, wrist veins, and thumb impressions). Unfortunately, equipment used in biometrics can lead to two types of errors: Type I and Type II. In practice, it is generally necessary to adjust the equipment for a compromise between false rejection of correct individuals (Type I error) and false acceptance of imposters (Type II error). The goal is to obtain low numbers for both types of errors. Equal error rate (crossover error rate) occurs when the false rejection rates and the false acceptance rates are equal.

EXAMPLES OF WEAK AND STRONG AUTHENTICATION METHODS

Examples of weak authentication methods include user IDs, PINs, and reusable (static and simple) passwords.

Examples of strong authentication methods include dynamic passwords (i.e., one-time passwords using challenge-response protocols), hardware tokens, passphrases, encrypted time stamps, smart cards, location-based authentication, memory cards, multiple factors of authentication, biometrics, and public key infrastructure (PKI) systems, such as digital signatures and digital certificates.

The principal forms of authentication include static, dynamic, and multiple factors.

- **Static authentication** reuses a specific authenticator (e.g., static password) where an attacker cannot obtain this authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authentication value.
- **Dynamic authentication** uses cryptography to create one per-session authenticator, and it changes with each authentication session between a claimant and verifier.
- **Multiple-factor authentication** requires two or more types of authentication techniques. It can include both static and dynamic authentication mechanisms. One example is the user of a password along with a smart card token.

Authorization mechanisms fall into several major categories, such as local, network, single sign-on, reduced sign-on, single log-in and single log-out, as follows:

- **Local authorization** is performed for each application and computer to which a user requires access. The local operating system and applications are employed to set up and maintain the authorizations for that computer or application.
- **Network authorization** is performed at a central, authorization server, providing access to a user's account from one or more workstations on the network and giving access to a single user account or multiple accounts. Security tokens (e.g., memory cards, flash memory, USB tokens, and smart cards) are used to allow access first to a computer and then to a network.
- **Single sign-on (SSO)** employs a central authorization server to enable a user to authenticate once and then access all the resources that the user is authorized to use. SSO achieves access to multiple applications, computers, workstations, and domains operating with a variety of authentication mechanisms (e.g., a Kerberos implementation used within a heterogeneous network). The central server establishes and maintains the authorizations at each application, computer, workstation, or domain that the user is allowed to access.
- **Reduced sign-on (RSO)** is a technology that allows a user to authenticate once and then access many, but not all, of the resources that the user is authorized to use.
- **Single log-in** is similar to single sign-on. It eliminates the need for authorization at each resource and for individual authentications to each resource.
- **Single log-out** is closing all open programs, files, functions, sessions, and screens with one system command so no computer resource is vulnerable to attackers.

(ii) Application Authentication Techniques for System Users

Organizational users include employees and outsiders, such as contractors. Users must uniquely be identified and authenticated for all accesses. Unique identification of individuals in group

accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of system user identities is accomplished through the use of passwords, tokens, biometrics, or, in the case of multifactor authentication, some combination thereof.

Access to systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access that involves communication through an external network (e.g., the Internet). Internal networks include LANs, WANs, and VPNs that are under the control of the organization. For a VPN, the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted.

Specific controls for system users are listed next.

- The system should use multifactor authentication for network access to privileged and nonprivileged accounts.
- The system should use multifactor authentication for local access to privileged and nonprivileged accounts.
- The organization should allow the use of group authenticators only when used in conjunction with an individual/unique authenticator and require individuals to be authenticated with an individual authenticator prior to using a group authenticator.
- The system should use multifactor authentication for network access to privileged and nonprivileged accounts where one of the factors is provided by a device separate from the information system being accessed.
- The system should use replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts. An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time-synchronous or challenge-response one-time authentication.
- The organization should conduct a risk assessment to determine the risks of identifying and authenticating nonorganizational users. Factors such as scalability, practicality, and security must be considered simultaneously to balance ease of use with protection.

(iii) Application Authentication Techniques for Devices

An information system should uniquely identify and authenticate specific types of devices before establishing a connection. Devices include mobile devices (e.g., USB memory sticks, external hard disk drives, notebook/laptop computers, cellular/mobile telephones, digital cameras, audio recording devices, and PDAs) and mobile ID devices (used to acquire fingerprint, face, and iris images in personal ID verification programs). These devices can use either shared known information (e.g., Media Access Control [MAC] or TCP/IP addresses) for identification or authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol, remote authentication dial-in user service [RADIUS] server with EAP-Transport Layer Security authentication, or Kerberos) to identify and authenticate devices on LANs, WANs, and wireless networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

General controls over devices are listed next.

- The information system should authenticate devices before establishing local network, remote network, and wireless network connections using bidirectional authentication between devices that is cryptographically based.
- Usage restrictions and operational guidance include proper configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection and firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system integrity checks, and disabling unnecessary hardware (e.g., wireless and infrared).
- Travel guidance for employees who are traveling includes providing computers with sanitized hard drives, limited applications, and additional hardening with stringent configuration settings. Security measures for employees who have returned from travel include examining the device for signs of physical tampering and purging or reimaging the hard disk drive.
- Regarding dynamic address allocation for devices, the organization should standardize Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices and audit lease information when assigned to a device. DHCP-enabled clients typically obtain **leases** for IP addresses from DHCP servers.
- Using the RADIUS protocol, a remote client can exchange authentication, access control, accounting, and device configuration information with a RADIUS server. The RADIUS server can authenticate a user or a device from its database or user I&A parameters.
- Using the Terminal Access Controller Access-Control System + (TACACS+) protocol enables a network resource to offload the user administration to a central server.

Specific controls over mobile devices are listed next.

- Smart card authentication (i.e., proof by possession)
- Password authentication (i.e., proof by knowledge)
- Fingerprint authentication (i.e., proof by property)

Specific controls over mobile ID devices are listed next.

- The data encryption algorithm should use Advanced Encryption System-256 (AES-256) for transmission and should provide for the encryption and decryption of bidirectional traffic.
- Data at rest should use encryption for all data residing on the device either as a temporary file or a part of the database.
- Data storage cards should use encryption for all of the device data, files, or databases written to storage medium.
- Biometric operator authentication should be achieved by a two-factor authentication, one of which should be a biometric.
- A password of minimum length with alphabetical, numerical, and/or special characters should be used for biometric operator authentication.

WHAT ARE USER AUTHENTICATORS AND DEVICE AUTHENTICATORS?

Examples of user authenticators include passwords, tokens, biometrics, PKI certificates, such as electronic signatures and digital certificates, and key cards.

Examples of device authenticators include passwords, and PKI certificates, such as electronic signatures and digital certificates.

- The device should provide the capability for biometric operator reauthentication after a designated length of time, the device should be reauthenticated itself after a designated amount of idle time or result in a device shutoff
- The device should provide the capability to lock the device or render it inoperable, erase selective file, and/or erase all files on it based on failed security protocols.
- The device should provide the capability to establish a maximum limit of failed authentication attempts before the handheld clears all application data or requires unlock only by a security administrator.
- After a biometric operator's authentication and authorization is established, the device's identification should be verified by matching against a list of specified devices (i.e., blacklists or lost/stolen lists). A matched device should not be authorized to communicate with the central system.
- All devices should be updated whenever policies change or software is updated to provide greater protection.
- When inserting a protected (encrypted) memory card into the mobile device's expansion slot, the device should be able to detect an encrypted card and prompt the biometric operator for the card's authentication code. Access to information would be granted only when the correct authentication code has been provided.
- The data authentication algorithm should use the Rivest, Shamir, Adelman-2048 (RSA-2048) key size. The secure hash function for the signature should use Secure Hash Algorithm (SHA-256) key size.

(iv) Identity Management and Privilege Management

Identity management is the comprehensive management and administration of user permissions, privileges, and profiles. It provides a single point of administration for managing the life cycle of accounts and profiles. **Identity** is the distinguishing character or personality of an individual based on a set of physical and behavioral characteristics by which that individual is uniquely recognized.

Access control ensures that only authorized access to resources occurs. It helps protect confidentiality, integrity, and availability and supports the principles of legitimate use, least privilege, and separation of duties. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses. Identity and access management ensures that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions.

In the past, users typically subscribed to each system or resource separately, as needed for their job functions, by undertaking multiple systems and user registration processes. This resulted in

users having to manage multiple security credentials (i.e., certificates, usernames, and passwords). This arrangement is tedious, expensive, time consuming, unattractive, and frustrating for users, as it scales poorly as the number of resources increases.

In light of these problems, a single solution is needed that allows user management processes to be efficiently and effectively leveraged and reused across trust domains, thereby facilitating interoperability between various information systems. This solution is accomplished through an access life cycle consisting of these five phases:

1. **Provisioning (vetting)** is a procedure for enabling end users to access and use system services. It involves creating for each user an account in a directory service and populating the account with the user-specific information needed by each service. It asks a question: What can you access?
2. **Permissioning** is the authorization given to users that enables them to access specific resources on the network, such as data files, applications, printers, and scanner. User permissions also designate the type of access, such as read only (view) or update only (read/write). It asks a question: What can you access?
3. **Credentialing** involves a certification authority issuing a certificate after validating an applicant who is requesting the access. It asks a question: How do I know it is you?
4. **Analyzing** is reviewing current accounts, old accounts, and expired accounts for correctness and appropriateness against their access rights and permissions.
5. **Revoking** includes canceling user accounts, expired accounts, and illegal accounts and decertifying users who are no longer valid, appropriate, or correct.

In addition, identity binding and identity proofing are required. **Identity binding** is tying the vetted claimed identity according to the credential-issuing authority, perhaps through biometrics. **Identity proofing** is the process by which a credential-issuing authority validates sufficient information (e.g., source documents, credentials, personal identification cards, and photo IDs) and validates them to uniquely recognize an individual.

Major benefits of identity and access management include providing single sign-on (SSO), reduced sign-on (RSO), and single logout (SLO) capabilities to end users for accessing multiple online systems and services. This will eliminate the need for registering end user identity information in multiple systems and services. This type of management is supported by several basic security technologies, including cryptographic trust model, identity management standards and middleware, and a metadata model for securely exchanging information about users.

Although the SSO system is designed for user convenience, cost savings, and efficiency, it can be subjected to a single point of failure due to concentration of risks in one place and at one time. Thus, if the SSO system is compromised, all the connected multiple systems can be compromised too.

Privilege management creates, manages, and stores the attributes and policies needed to establish criteria that can be used to decide whether an authenticated entity's request for access to some resource should be granted. Enterprise-level privilege management fits under the umbrella of enterprise-level access control. At the enterprise level, access management encompasses all the practices, policies, procedures, data, metadata, and technical and administrative mechanisms

used to manage access to the resources of an organization. Access management includes access control, privilege management, and identity management, as shown:

Access management = Access control + Privilege management + Identity management

Access control ensures that resources are made available only to authorized users, programs, processes, or systems by reference to rules of access that are defined by attributes and policies. In privilege management, resources can be both computer-based objects (e.g., files and Web pages) and physical objects (e.g., buildings and vault safes). The entities requesting access to resources can be users (people) and processes running on a computer, application, or system. Identity management deals with identification and authentication, authorization, decision, and enforcement processes.

(v) Integrating Identification and Authentication Methods

Four-factor authentication methods have been proven stronger and better than single-factor authentication methods, shown next.

*One-Factor Authentication Method***.** Any one of the following can represent a one-factor authentication method, which is not strong and secure.

- Something you have (e.g., photo ID, memory card, smart card, PIV card with PIN for swiping into a reader with photo, decal mounted onto a motorized vehicle, transponder mounted on a motorized vehicle used for operating an automated entry point, visitor badge without name and photo, physical key, digital certificate, hardware token, and mobile ID device).
- Something you know (e.g., password or PIN; shared or unshared combination, such as electronic safe, cipher lock, PIN pad combination, and digital certificate).
- Something you are (e.g., photo ID, PIV card with PIN or photo, fingerprint identification [one-to-many], fingerprint verification [one-to-one], hand geometry [one-to-many], iris scan [one-to-many], colleague [peers and coworkers] recognition, and user [peers or security guards] recognition). Colleague and user recognitions are considered attended access.
- Somewhere you are (e.g., geodetic location, such as a building, city, sate, or country using a GPS) for employees traveling to and from the company's remote location or to and from vendor/customer location.

*Two-Factor Authentication Methods***.** Any one of the following can represent a two-factor authentication method. Note that there are many combinations due to use of several authentication devices.

- Combination of something you have and something you know (e.g., digital certificate where digital signature is used with PIN to unlock the private key; cryptographic hardware token with one-time password device and PIN; and PIV card with PIN or password for after-hours entry without after-hours attendant).
- Combination of something you have and something you are (e.g., verified digital or optical photo ID with driver's license and personal identity card with photo or attended/unattended access, hardware token with biometrics).
- Combination of something you know (e.g., user ID, PIN, and passwords) and something you are (e.g., biometric sample).

- Combination of something you have, something you know, and something you are (e.g., personal identity card with attended access and PIN). This combination is an attended or two-person access control method using the card and the PIN and is not the strongest two-factor authentication because of the attendant.
- Combination of something you have (1), something you have the same as in (1) (2), and something you know (e.g., PIV card and digital certificate). This combination illustrates that multiple instances of the same factor (i.e., something you have) results in two-factor authentication. However, this implementation represents a higher level of assurance than other instances of two-factor authentication. Two factor is better than one factor.

Three-Factor Authentication Methods. Combination of something you have (i.e., public key infrastructure (PKI) keys or a hardware token), something you know (i.e., PIN or password), and something you are (i.e., comparing the cardholder to the biometric image stored on the biometric database and/or on the access card) represents the strongest three-factor authentication. A hardware token can be used in support of this level of assurance in logical access control. Three-factor is better than one-factor and two-factor methods.

Four-Factor Authentication Methods. Combination of something you have (i.e., card, key, or mobile ID device), something you know (i.e., PIN or password), something you are (i.e., fingerprint or signature), and something about where you are (i.e., building or company/remote location, or vendor/customer location) represents the strongest and highest form of all authentication methods.

(e) Encryption

In this section, foundational concepts; methods, types, modes, and alternatives to encryption; basic types of cryptographic key systems; basic uses of cryptography; digital signatures, digitized signatures, electronic signatures, and digital certificates; cryptographic methods to protect data at rest and data in transit; and alternatives to cryptography are discussed.

(i) Foundational Concepts

Cryptography is the science of transforming data so that it is interpretable only by authorized persons, and it involves encryption and decryption methods in transforming such data. **Encryption** is disguising plaintext results in ciphertext (i.e., encrypted data). **Decryption** is the process of transforming ciphertext back into plaintext (i.e., unencrypted data). This means that the original process is encryption and the reverse process is decryption. Cryptography and encryption are related in that encryption technologies are used in the cryptographic transformation of plaintext data into ciphertext data to conceal the data's original meaning to prevent it from being known or used. When interception, theft, or destruction is a likely threat to information, encryption provides an additional layer of protection.

The relationship among cryptology, cryptography, and cryptanalysis is as follows:

$$\text{Cryptology} = \text{Cryptography} + \text{Cryptanalysis}$$

Cryptology is the field that encompasses both cryptography and cryptanalysis. It is the science that deals with hidden, disguised, or encrypted communications. It embraces communications security and communication intelligence.

Cryptography relies on two basic components: an algorithm and a key. **Algorithms** are complex mathematical formulas, and **keys** are strings of bits used in conjunction with algorithms

to make the required transformations. For two parties to communicate, they must use the same algorithm(s) that are designed to work together. In most cases, algorithms are documented, and formulas are available to all users, although the algorithm details are sometimes kept secret. Some algorithms can be used with keys of various lengths. The greater the length of the key used to encrypt the data, the more difficult it is for an unauthorized person to use a trial-and-error approach to determine the key and successfully decrypt the data.

Cryptanalysis is the steps and operations performed in converting encrypted messages into plaintext without initial knowledge of the key employed in the encryption algorithm.

Encryption or cryptography is a method of converting information to an unintelligible code. The process can then be reversed, returning the information to an understandable form. The information is encrypted (encoded) and decrypted (decoded) by what are commonly referred to as cryptographic keys. These "keys" are actual values used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected.

Because encryption renders information unreadable to any party without the ability to decrypt it, the information remains private and confidential, whether transmitted or stored on a computer system. Unauthorized parties will see nothing but an unorganized assembly of characters. Furthermore, encryption technology provides data integrity assurance as some algorithms offer protection against forgery and tampering. The ability of the technology to protect information requires that authorized parties properly manage the encryption and decryption keys.

(ii) Methods of Encryption

In general, the encryption mechanism effectively seals the information within an object inside an additional (logical) container. Used primarily to provide confidentiality, general encryption can be used to ensure the detection of integrity violations and to otherwise hinder integrity attacks. Encryption is not absolute protection, as the sealing process may be only as safe as the encryption key. Also, encryption of an object does not in and of itself prevent damage to its integrity. However, encryption does provide an additional level of protection that must be circumvented in order to violate protection policies or to succeed at making violations without detection. Distinct advantages of encryption are its flexibility of use, which includes its ability to be used either as blanket protection or "on demand," and its applicability to a wide array of object types. For example, digital signatures are intended to produce the same effect as a real signature, an unforgettable proof of authenticity.

The four major methods of encryption include one-time pads, substitution ciphers, transposition ciphers, and substitutions and permutations.

1. **One-time pads.** A one-time pad is unbreakable given infinite resources. It is a large nonrepeating set of truly random key letters. Each cipher key is used exactly once, for only one message. The sender encrypts the message and then destroys the pad's pages. The receiver does the same thing after decrypting the message. A requirement is that the key letters have to be generated randomly. Any attacks will target the method used to generate the key sequence. An advantage is that one-time pads are used in ultra-secure and low-bandwidth channels, hence provide security over the transmitted key. A disadvantage is that they require an amount of key information equal to the size of the plaintext being enciphered.

2. **Substitution ciphers.** In a substitution cipher, each letter or group of letters is replaced by another letter or group of letters to disguise it. Probable words or phrases are guessed. Substitution ciphers preserve the order of the plaintext symbols but disguise them. Substitutions are performed by substitution boxes (S-boxes).
3. **Transposition ciphers.** In contrast to substitution ciphers, transposition ciphers reorder the letters but do not disguise them. The cipher is keyed by a word or phrase not containing any repeated letters. Permutation boxes (P-boxes) are used to effect a transposition.
4. **Substitutions and permutations.** An S-box is a nonlinear substitution table box used in several byte substitution transformations and in the key expansion routine to perform a one-for-one substitution of a byte value. S-boxes are used in the Advanced Encryption Standard (AES). Cipher keys are used in various permutations and combinations to keep the encryption scheme much stronger and highly secure. DES is not secure.

(iii) Types of Encryption

There are at least three types of encryption: stream ciphers, block ciphers, and product ciphers.

(A) Stream Ciphers Stream ciphers are algorithms that convert plaintext to ciphertext one bit at a time. Their security depends entirely on the insides of the key-stream generator. Because it is necessary to change the key with each message, stream ciphers are not usually used to encrypt discrete messages. They are useful in encrypting nondiscrete messages, such as a T-1 link between two computers. In other words, they are good for continuous streams of communication traffic. The key-stream generator produces the same output on both the encryption and decryption ends.

There are three variants of stream ciphers: synchronous stream ciphers, self-synchronous stream ciphers, and using block ciphers as stream ciphers. In a synchronous stream cipher, the key-stream is generated independent of the message stream and is vulnerable to an **insertion attack**. **A countermeasure** is to not use the same key-stream to encrypt two different messages. In a self-synchronous stream cipher, each key-stream bit is a function of a fixed number of previous ciphertext bits. In the third variant, the block cipher algorithms are used as key-stream generators. Protocols that use stream ciphers with no-cryptographic checksums (e.g., Cyclical Redundancy Checks-32 [CRC-32]) are vulnerable to attacks.

The major characteristics of stream ciphers are listed next.

- They are not suitable for software implementation due to time-consuming manipulation of bits.
- They are easier to analyze mathematically than block ciphers.
- A single error can damage only a single bit of data.
- A good application is a T-1 link between two computers.
- A key-stream reuse attack is possible when the same key and initialization vector pair is used twice.

(B) Block Ciphers A block cipher is a family of functions and their inverse functions that are parameterized by cryptographic keys. The functions map bit strings of a fixed length to bit strings of the same length. Several modes of operation are used with symmetric key block cipher algorithms.

Major characteristics of block ciphers are listed next.

- They are easy to implement in software due to less time consumption.
- They are more general in use.
- Algorithms are stronger.
- A single error can damage a block's worth of data.
- A good application is data on a computer.
- They take an *n*-bit block of plaintext as input and transform it using the key into an *n*-bit block of ciphertext.
- They are subject to cryptanalysis attacks, such as differential and simple power analysis and timing analysis.

(C) Product Ciphers Product ciphers are a whole series of combinations of P-boxes and S-boxes cascaded. In each iteration, or round, first there is an S-box followed by a P-box. In addition, there is one P-box at the beginning and one P-box at the end of each round. Common product ciphers operate on k-bit inputs to product k-bit outputs. P-boxes and S-boxes can be implemented on hardware with electrical circuits.

(iv) Modes of Encryption

There are basically two modes of encryption in a network: link (online) encryption and end-to-end encryption. It is possible to combine both modes of encryption.

Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line), including headers, addresses, and routing information. Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing.

WHO PERFORMS LINK ENCRYPTION AND END-TO-END ENCRYPTION?

- Data communications service providers generally perform link encryption.
- End user organizations generally perform end-to-end encryption.
- Link encryption occurs at the lower levels of the ISO/OSI model and encrypts both headers and trailers of the packet.
- End-to-end encryption occurs at the higher levels of the ISO/OSI model and does not encrypt headers and trailers.

Link encryption provides good protection against external threats, such as traffic analysis, because all data flowing on links can be encrypted, thus providing traffic-flow security. Entire packets are encrypted on exit from and decrypted on entry to a node. Link encryption also protects against packet sniffing and eavesdropping threats. Link encryption is easy to incorporate into network protocols.

However, link encryption has a major disadvantage: A message is encrypted and decrypted several times. If a node is compromised, all traffic flowing through that node is also compromised. A secondary disadvantage is that the individual user loses control over algorithms used. Another disadvantage is that key distribution and management is more complex.

In **end-to-end encryption**, a message is encrypted and decrypted only at endpoints, thereby largely circumventing problems that compromise intermediate nodes. However, some address information (data link headers and routing information) must be left unencrypted to allow nodes to route packets. Although data remains encrypted when being passed through a network, header and routing information remains visible. High-level network protocols must be augmented with a separate set of cryptographic protocols.

(v) Alternatives to Encryption

Full disk, virtual disk and volume, and file/folder encryption technologies are used for storage encryption on end user devices. Many other acceptable alternative methods to encryption are available to achieve the same objective. Alternatives include using:

- Backup utility programs to encrypt backups.
- Compression utility programs to encrypt archives.
- Cryptographic hashes of passwords instead of regular passwords.
- Digital rights management (DRM) software to restrict access to files.
- Virtual machines (VMs) to access and store sensitive information.

Sometimes the best way to address the problem of protecting sensitive information on end user devices is not to store the information on higher-risk devices (e.g., mobile devices or removable media) and to remove unneeded sensitive information from files or databases. If certain network traffic does not need to be encrypted or should not be encrypted, then other security controls such as IDS sensors can monitor the contents of traffic.

Other alternative approaches to encryption include:

- Using a **thin client** solution, such as terminal services, a thin Web-based application, or a portal to access the information and configuring the thin client solution to prohibit file transfers of the sensitive information to the end user device.
- Configuring the organization's devices, including desktop computers, to prevent writing sensitive information to removable media (e.g., compact disks, flash drives, flash drives, thumb drives, or pen drives) unless the information is properly encrypted.

(vi) Basic Types of Cryptographic Key Systems

Cryptography relies on two basic components: an algorithm and a key. Algorithms are complex mathematical formulae and keys are strings of bits. For two parties to communicate, they must use the same algorithm(s). In some cases, they must also use the same key. Most cryptographic keys must be kept secret; sometimes algorithms are also kept secret.

There are two basic types of cryptographic key systems: secret or private key systems (also called symmetric key systems) and public key systems (also called asymmetric key systems). Often the two are combined to form a hybrid system to exploit the strengths of each type. The type of key that is needed depends on security requirements and the operating environment of the organization. See Exhibit 6.5 for basic types of cryptographic key systems.

(A) Secret Key System In a secret (private) key system, two (or more) parties share the same key, and that key is used to encrypt and decrypt data. If the key is compromised, the security offered by cryptography is severely reduced or eliminated. Secret key cryptography assumes that the parties

Secret (private) key system (uses a single key, shared by parties, also called symmetric key system [e.g., DES, 3DES, and AES])

Public key system (uses two keys, both private and public, not shared by parties, also called asymmetric key system [e.g., RSA, DSS, and DH])

Hybrid key system (combines the best of secret and public key systems)

EXHIBIT 6.5 Types of Cryptographic Key Systems

who share a key rely on each other to not disclose the key and to protect it against modification. Note that secret key systems are often used for bulk data encryption. The best-known secret key system is DES, which is used as the basis for encryption, integrity, access control, and key management standards.

The primary *advantage* of a secret key system is speed. Popular secret key encryption methods are significantly faster than any currently available public key encryption method. Alternatively, public-key cryptography can be used with secret-key cryptography to get the best of both worlds—the security advantages of public key systems and the speed advantages of secret key systems. The public key system can be used to encrypt a secret key used to encrypt the bulk of a file or message.

In some situations, public key system is not necessary, and secret-key system alone is sufficient. This includes computing environments where (1) a secure secret key agreement can take place, (2) a single authority knows and manages all the keys, and (3) there is a single user. In general, public key system is best suited for an open multi-user environment.

(B) Public Key System Whereas a secret key system uses a single key shared by two (or more) parties, a public key system uses a pair of keys for each party. One of the keys of the pair is public and the other is private. The public key can be made known to other parties; the private key must be kept confidential and must be known only to its owner. Both keys, however, need to be protected against modification. Note that public key systems are used for automated key distribution.

The public key system is particularly useful when the parties wishing to communicate cannot rely on each other or do not share a common key. Examples of public key systems include RSA and the Digital Signature Standard (DSS). **Zero-knowledge proof** is used in the public key system.

The primary advantage of the public key system is increased security and convenience; private keys never need to be transmitted or revealed to anyone. In a private, secret key system, the secret keys must be transmitted, either manually or through a communication channel. There may be a chance that an unauthorized individual can access the secret keys during their transmission.

(C) Strengths and Weaknesses of Private Keys and Public Keys A computer system can use both types of keys (private and public) in a complementary manner, with each performing different functions. Typically, the speed advantage of secret key (private key) cryptography means that it is used for encrypting bulk data.

Although public key cryptography does not require users to share a common key, secret key cryptography is much faster. Public key cryptography is used for applications that are less demanding

Distinctive Features	Private Keys	Public Keys
Number of keys	Single key shared by two or more parties	Pair of keys for each party
Types of keys	Key is secret	One key is private and one key is public
Protection of keys	Disclosure and modification	Disclosure and modification for private keys and modification for public keys
Relative speeds	Faster	Slower
Performance	Protocols are more efficient	Protocols are less efficient
Key length	Fixed key lengths	Variable key lengths
Application	Ideal for encrypting files and communication channels	Ideal for encrypting and distributing keys and for providing authentication

EXHIBIT 6.6 Strengths and Weaknesses of Private and Public Keys

to a computer system's resources, such as encrypting the keys used by secret key cryptography for distribution or to sign messages. Exhibit 6.6 compares the strengths and weaknesses of private keys with public keys.

(vii) Basic Uses of Cryptography

Cryptography creates a high degree of trust in the electronic world. It is used to perform five basic security services: confidentiality, data integrity, authentication, authorization, and nonrepudiation.

(A) Confidentiality Confidentiality is the property whereby information is not disclosed to unauthorized parties. Secrecy is a term that is often used synonymously with confidentiality. Confidentiality is achieved using encryption to render the information unintelligible except by authorized entities. The information may become intelligible again by using decryption. In order for encryption to provide confidentiality, the cryptographic algorithm and mode of operation must be designed and implemented so that an unauthorized party cannot determine the secret or private keys associated with the encryption or be able to derive the plaintext directly without deriving any keys.

(B) Data Integrity Data integrity is a property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. This includes the insertion, deletion, and substitution of data. Cryptographic mechanisms, such as message authentication codes or digital signatures, can be used to detect (with a high probability) both accidental modifications (e.g., modifications that sometimes occur during noisy transmissions or by hardware memory failures) and deliberate modifications (unauthorized alterations) by an adversary with a very high probability. Noncryptographic mechanisms are also often used to detect accidental modifications but cannot be relied on to detect deliberate modifications.

(C) Authentication Authentication is a service that is used to establish the origin of information. That is, authentication services verify the identity of the user or system that created information (e.g., a transaction or message). This service supports the receiver in security-relevant decisions, such as "Is the sender an authorized user of this system?" or "Is the sender permitted to read sensitive information?" Several cryptographic mechanisms may be used to provide authentication services. Most commonly, authentication is provided by digital signatures or message authentication codes; some key agreement techniques also provide authentication. When multiple individuals are permitted to share the same authentication information (such as a password or cryptographic key), it is sometimes called role-based authentication.

WHAT ARE THE MAJOR USES AND TYPES OF CRYPTOGRAPHY?

Cryptography is used to provide confidentiality, data integrity, authentication, authorization, and nonrepudiation security services. Two basic types of cryptography exist: symmetric and asymmetric. Each has its own strengths and weaknesses. Most current cryptographic applications combine both types of cryptography (hybrid cryptography) to exploit the strengths of each type.

(D) Authorization Authorization is concerned with providing an official sanction or permission to perform a security function or activity. Normally, authorization is granted following a process of authentication. A noncryptographic analog of the interaction between authentication and authorization is the examination of an individual's credentials to establish his or her identity (authentication); upon proving identity, the individual is then provided with the key or password that will allow access to some resource, such as a locked room (authorization). Authentication can be used to authorize a role rather than to identify an individual. Once authenticated to a role, an entity is authorized for all the privileges associated with the role.

(E) Nonrepudiation Nonrepudiation is a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party. This service prevents an entity from successfully denying involvement in a previous action. Nonrepudiation is supported cryptographically by the use of a digital signature that is calculated by a private key known only by the entity that computes the digital signature.

(viii) Digital Signatures, Digitized Signatures, Electronic Signatures, and Digital Certificates

A digital signature is an electronic analog of a handwritten signature in that it can be used to prove to the recipient, or a third party, that the originator in fact signed the message. Digital signatures are also generated for stored data and programs to verify data and program integrity at any later time.

Digital signatures authenticate the integrity of the signed data and the identity of the signatory. They verify to a third party that data were actually signed by the generator of the signature. Digital signatures are used in e-mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications requiring data integrity assurance and data origin authentication. Digital signatures can address potential threats, such as spoofing, masquerading, replay attacks, and password compromise. They cannot address denial-of-service (DoS) attacks.

The security of a digital signature system is dependent on maintaining the secrecy of users' private keys. Users must, therefore, guard against the unauthorized acquisition of their private keys. A digital signature can also be used to verify that information has not been altered after it was signed; this provides message integrity. A simpler alternative to a digital signature is a hash function.

Digital signatures offer protection not available by alternative signature techniques, such as a **digitized signature**. Converting a visual form of a handwritten signature to an electronic image generates a digitized signature. Although a digitized signature resembles its handwritten counterpart, it does not provide the same protection as a digital signature. Digitized signatures can be forged as well as duplicated and appended to other electronic data. Digitized signatures cannot be used to determine whether information has been altered after it is signed.

An **electronic signature** is a cryptographic mechanism that performs a function similar to a handwritten signature. It is used to verify the origin and contents of a message.

ELECTRONIC SIGNATURES VERSUS HANDWRITTEN SIGNATURES

Electronic signatures are very difficult to forge, although handwritten signatures are easily forged. In general, electronic signatures have received the same legal status as that of written signatures. Cryptography can provide a means of linking a document with a particular person, as is done with a written signature. If a cryptographic key is compromised due to social engineering attack, then the electronic originator of a message may not be the same as the owner of the key. Trickery and coercion are problems for both electronic and handwritten signatures (i.e., social engineering attacks).

Digital certificates are basically containers for public keys and act as a means of electronic identification. The certificate and public keys are public documents that, in principle, anyone can possess. An associated private key, possessed only by the entity to which the certificate was issued, is used as a means of binding the certificate to that entity. Users not possessing this private key cannot use the certificate as a means of authentication. Entities can prove their possession of the private key by digitally signing known data or by demonstrating knowledge of a secret exchanged using public key cryptographic methods. A digital certificate is a password-protected and encrypted file. It should not contain any owner-related information that changes frequently. In practice, anyone can generate public–private key pairs and digital certificates; consequently, it is necessary to determine whether the certificate holder is trustworthy.

(ix) Cryptographic Mechanisms to Protect Data at Rest

The scope of data at rest, data in storage, or data on a hard-drive includes protecting the confidentiality, integrity, and availability of data residing on servers, workstations, computers, storage/disk arrays (e.g., RAID), network attached storage appliances, disk drives, tape drives, and removable media such as flash drives, thumb drives, and pen drives.

The need for encrypting the storage media is increasing, and selecting an encryption algorithm with the right strength is important to protect the media from internal and external attacks. Use of encryption algorithms (e.g., DES and 3DES) and hashing algorithms (e.g., MD5 and SHA-1) are considered to be no longer secure. Encrypting the storage media with AES-256 and providing end-to-end security is advised due to its strong and secure algorithm. When using AES-256, do not store the encryption keys in cleartext or leave them in an open operating system because the keys can be compromised.

Cryptographic mechanisms to protect data at rest include storage encryption technologies, such as full (whole) disk encryption, virtual disk encryption, volume encryption, file encryption, and/or folder encryption. Information stored on end user devices can be encrypted in many ways. For example, an application that accesses sensitive information could be responsible for encrypting that information. Applications such as backup programs might also offer encryption options. Another method for protecting files is digital rights management (DRM) software.

Technologies such as firewalls, intrusion prevention systems, and virtual private networks (VPNs) seek to secure data by protecting the perimeter of the network. Unfortunately, these technologies do not adequately secure data in storage, as data is still stored in cleartext and thus is open to a wide range of internal and external attacks. Encrypting data at rest on tape and disk will mitigate such attacks and secure data while maintaining the current service levels.

Adding encryption to data at rest poses some challenges, such as changing the application code, data compression problems, slow response time, user unfriendliness, complexity, and additional

cost to storage systems. The other challenge includes the impact of encryption on cryptographic key management. For example, keys:

- Can be lost, resulting in loss of data.
- Need to be kept secure but should be available.
- Have to be retained until the data is retained.
- Need to be created, changed, or destroyed.
- Need to be managed without excessive operational and administrative complexity.

Storage encryption can be applied as a part of data-at-rest solution in several places. For example, encryption can be used:

- In the application.
- In the file system or operating system.
- In the device driver or network interface.
- On the network.
- In the storage controller.
- In the storage device using a single-factor authentication (e.g., password, user ID, or, hardware token) and multiple-factor authentication (e.g., password, user ID, smart card, or cryptographic token).

(x) Cryptographic Mechanisms to Protect Data in Transit

The scope of data in transit, data in flight, or data on the wire includes protecting the confidentiality, integrity, and availability of data as it is transferred across the storage network, LAN, and WAN.

Cryptographic mechanisms in controlling data in transit through remote access to an information system are listed next.

- Use encryption with a strong key in relation to the security categorization of the information.
- Restrict execution of privileged commands.
- Use standard bulk or session layer encryption, such as SSH and VPNs with blocking mode enabled.
- Route all remote accesses through a limited number of managed access control points.
- Do not use Bluetooth and peer-to-peer networking protocols because they are less secure.

(xi) Alternatives to Cryptography

There are at least three alternatives methods to cryptography in order to hide information: steganography, digital watermarking, and reversible data hiding.

- **Steganography** (concealed writing) deals with hiding messages and obscuring who is sending or receiving them. It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, which provides a form of security through obscurity.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion and may be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Media files are ideal for steganographic transmission because of their large sizes and the fact that changes are so subtle that someone not specifically looking for them is unlikely to notice them.

- **Digital watermarking** is a type of marking that embeds copyright information about the copyright owner. Digital watermarking is the process of irreversibly embedding information into a digital signal.

  Steganography is sometimes applied in digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself.

  A digital watermark is called robust with respect to transformations if the embedded information can reliably be detected from the marked signal even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression are often added to this list.

  A digital watermark is called imperceptible if the cover signal and marked signal are indistinguishable with respect to an appropriate perceptual metric. In general, it is easy to create robust or imperceptible watermarks, but the creation of robust and imperceptible watermarks has proven to be quite challenging. Robust and imperceptible watermarks have been proposed as tool for the protection of digital content—for example, as an embedded "no-copy-allowed" flag in professional video content.

- **Reversible data hiding** is a technique that enables images to be authenticated and then restored to their original form by removing the watermark and replacing the image data that had been overwritten. This method would make the images acceptable for legal purposes.

SUMMARY OF ENCRYPTION METHODS

- In link encryption, all data including addresses flowing on links can be encrypted.
- In end-to-end encryption, a message is encrypted and decrypted only at endpoints by hardware and software techniques.
- Bulk (trunk) encryption is simultaneous encryption of all channels of a multichannel telecommunications trunk. No bulk encryption is needed when a public key cryptographic is used to distribute keys since the keys are generally short.
- Session encryption is used to encrypt data between applications and end users. It is effective in preventing an eavesdropping attack from remote access to firewalls. A secure server supports server authentication and session key encryption.

- Stream encryption encrypts and decrypts messages of arbitrary sizes.
- Line encryption protects data in transfer, which can be used to achieve confidentiality.
- File encryption protects data in storage. It is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.
- Field-level encryption is stronger than file-, record-, and packet-level encryption.
- Folder encryption is the process of encrypting individual folders on a storage medium and permitting access to the encrypted files within the folders only after proper authentication is provided.
- Full (whole) disk encryption is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product is made.
- Virtual disk encryption is the process of encrypting a container, which can hold many files and folders, and permitting access to the data within a container only after proper authentication is provided.
- Volume encryption is the process of encrypting an entire volume and permitting access to the data on the volume only after proper authentication is provided.
- Multiple (e.g., triple) encryption is stronger than single encryption but costs may increase and system performance may decrease.
- NULL encryption is used when integrity protection is required for an (Internet Protocol security (IPsec) system, not for confidentiality.
- Super-encryption is a process of encrypting information that is already encrypted. It occurs when a message, encrypted offline, is transmitted over a secured, online circuit or when information encrypted by the originator is multiplexed onto a communication trunks, with the information then bulk encrypted. In other words, super-encryption is encryption plus encryption and from offline to online.

6.2 Application Development

(a) Systems Development Methodology

In this section, approaches to develop or acquire information systems or application systems are presented. In addition, models deployed in and tools to be applied in software development are discussed. The need for conducting due care and due diligence reviews during system development or acquisition is highlighted.

(i) Traditional Approaches to Develop or Acquire Systems

Two approaches or methodologies exist to develop or to acquire information systems or application systems: traditional approaches and alternative approaches. The traditional approach requires systematic and disciplined work using a system development life cycle (SDLC) methodology with phases to ensure consistency and quality of work. Five phases of SDLC include the following:

1. Planning/initiation
2. Development/acquisition
3. Implementation/assessment

4. Operation/maintenance
5. Disposal/decommissioning

Usually, the traditional approach combined with the SDLC methodology is used in developing custom software. Next, system-related activities and security-related activities are presented for each phase of the SDLC.

(A) Phase 1: Planning/Initiation System-related activities are listed next.

- Understanding a functional user's request for a new system
- Conducting a feasibility study (i.e., costs and benefits)
- Performing high-level needs assessment
- Doing a preliminary risk assessment
- Using decision tables, flowcharts, data-flow diagrams, and finite-state-machine models to express user needs and system requirements

Security-related activities include developing the security-planning document, conducting a sensitivity assessment, and security assurance (cost driver). The security-planning document contains several elements, such as those listed next.

- Security awareness and training plans
- Rules of behavior
- Risk assessment
- Configuration management (CM) plan
- Contingency plan
- Incident response plan
- System interconnection agreements
- Security tests and evaluation results
- Plan of actions and milestones

However, the security-planning document does not contain a request for proposal, vendor contract plans, or a statement of work, as they are related to project management, not to security management.

(B) Phase 2: Development/Acquisition System-related activities are listed next.

- Performing an in-depth analysis of user needs
- Performing general and detailed system design work
- Developing computer programs
- Conducting unit and system testing
- Planning desk reviews, mutation analysis, sensitivity analysis for analyzing changes, boundary-value analysis, and error seeding methods during testing

- Performing quality assurance (QA) and quality control (QC) reviews
- Doing a detailed risk assessment

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

Security-related activities are listed next.

- Determining security features, controls, assurances, and operational practices
- Incorporating these security requirements into security design specifications
- Actually building or buying these security requirements into the system
- Conducting design reviews through walk-throughs
- Preparing test documents with test cases and test procedures with formal specific programming languages
- Conducting certification and accreditation activities

Possible security threats or vulnerabilities that should be considered during this phase include Trojan horses, incorrect/incomplete program code, poorly functioning software development tools, manipulation of program code, and malicious insiders.

(C) Phase 3: Implementation/Assessment System-related activities are listed next.

- Providing training to end users and system users
- Conducting acceptance testing for end users
- Converting the old system into the new system
- Developing instruction manuals for system use
- Performing QA and QC reviews

After acceptance testing and conversion, the system is installed or fielded with a formal authorization from management to put into production status.

Security-related activities include installing or turning on security controls, performing security tests (e.g., functional tests, penetration tests), and security evaluation report and accreditation statement.

(D) Phase 4: Operation/Maintenance System-related activities are listed next.

- Doing production operations and support work
- Performing a postimplementation review
- Undertaking system maintenance and modification work
- Monitoring the system's performance

During this phase, the system is fully operational and doing its work as intended and planned. The system is frequently modified by the addition of new hardware and software and by new functional requirements. The CM process is implemented with baselines and change controls.

Security-related activities are listed next.

- Security operations and administration (e.g., performing backups, managing cryptographic keys, setting user access accounts, and updating security software)
- Operational assurance (e.g., conducting system audits and continuous monitoring)
- Periodic reaccreditation when security is insufficient and when the changes made are significant

WHAT IS THE FOCUS OF SYSTEM REQUIREMENTS, DESIGN, AND IMPLEMENTATION IN SYSTEM DEVELOPMENT?

- System requirements describe external behavior of a computer system. They focus on what the software is to accomplish. Requirements present unmet user needs and unsolved business problems.
- System design describes the internal behavior of a computer system. It focuses on how to develop a solution to unmet user needs and business problems. Design satisfies user needs and solves business problems.
- System implementation focuses on how to use and operate the software.

(E) Phase 5: Disposal/Decommissioning System-related activities include system retirement or replacement plans and media sanitization procedures. The computer system is disposed of (terminated) once the transition to a new computer system is completed.

Security-related activities are listed next.

- Disposition of information (i.e., data sanitization), hardware, and software
- Moving information to archives after considering legal and audit requirements for records retention and the method of retrieving the information in the future
- Disposition of software after considering licensing terms and agreements (site-specific) with the developer, if the agreement prevents the software from being transferred
- Taking appropriate steps to ensure secure long-term storage of cryptographic keys and for the future use of data if the data have been encrypted

Some organizations may not have software disposal or decommissioning policies and procedures; in other organizations, such procedures might have been overlooked. Software acquirers should ensure that such policies and procedures are developed and followed to ensure the safe and secure disposal or decommissioning of software and to ensure that data are destroyed or migrated safely and securely. When a software-intensive system is retired or replaced, the data must be migrated by validated means to the new software-intensive system or must be made unreadable before disposal. Note that encrypted data may not be adequately protected if they are weakly encrypted. *Simply stated, residual data equals residual risk.*

Another consideration in this phase concerns storage devices used in virtualization process. Before a device using a virtualization process permanently leaves an organization (such as when a leased server's lease expires or when an obsolete personal computer [PC] is being recycled), the organization should remove any sensitive data from the host. Data may also need to be wiped if

an organization provides loaner devices to teleworkers, particularly for travel. Note that sensitive data may be found nearly anywhere on a device because of the nature of virtualization. For this reason, an organization should strongly consider erasing all storage devices completely.

Another related concern in this phase is removing or destroying any sensitive data from the Basic Input/Output System (BIOS) to reduce the chances of accidental data leakage. The configuration baseline should be reset to the manufacturer's default profile; in particular, sensitive settings, such as passwords, should be deleted from the system and cryptographic keys should be removed from the key store.

(ii) Models in System Development

Several models exist to either develop or acquire information systems, and each model may be suitable to a particular environment. In practice, a combination of these models may be deployed after considering the time, cost, and skills constraints and trade-offs.

- The **waterfall model** takes a linear, sequential view of the software engineering process, similar to an SDLC model.
- The **rapid application development (RAD) model** is quite opposite to the waterfall model. That is, it is good when requirements are not fully understood by both parties. It uses integrated computer-aided software engineering (I-CASE) tools and fourth-general programming languages (4GLs) to quickly prototype an information system. Often software is reused in RAD.
- Although the **incremental development model** and the evolutionary development models are better than the waterfall model, they are not as good as rapid prototyping in terms of bringing the operational viewpoint to the requirements specification. Successive versions of the system are developed reflecting constrained technology or resources.
- The **spiral model** is another type of evolutionary model. It has been developed to provide the best feature of both the classic life cycle approach and prototyping.
- The **rapid prototyping model** is a process that enables the developer to create a model of the software built in an evolutionary manner. Rapid prototyping uses special software and a special output device to create prototype to design and test a system in three dimensions.
- The **object-oriented development model** is applied once the design model has been created. The software developer browses a library or repository that contains existing program components to determine if any of the components can be used in the design at hand. If reusable components are found, they are used as building blocks to construct a prototype of the software.

(iii) Tools in Systems Development

At least three tools exist to development systems quickly and completely, including prototyping, cleanroom software engineering, and computer-aided software engineering.

(A) Prototyping Defining software requirements is the biggest and most troublesome area to handle and control for functional users, information technology (IT) staff, and auditors. Yet it is the foundation upon which the entire applications software system is built. It is a very simple concept to grasp. If software requirements are incompletely defined and documented, the final product will be incomplete.

A major problem with software requirements is that the software development staff is working against a moving target because software requirements are constantly changing due to functional users' inability to define their requirements clearly and completely, communication problems between functional users and IT staff, and natural changes in business functional requirements over the time frame of the software development project from internal and external sources.

Defining software requirements is often taken very lightly; most of the time, the step is skipped or skimped on. Consequently, excessive maintenance of software is needed after the system becomes operational to meet the missing requirements, which should have been addressed earlier.

PROTOTYPING VERSUS COMMUNICATION

Prototyping increases communication between people, which is often the major problem in the traditional definition and documentation of software requirements.

An approach that rapidly brings a working version of the system into the hands of the user seems to be a better strategy. This is because users sometimes cannot actually define system requirements correctly the first time until they have used some or all parts of the system. Prototyping is one way of dealing with the uncertainty, impreciseness, inconsistency, difficulty, and ambiguity involved in defining software requirements and design work. User requirements are not frozen; in fact, changing of users' minds is welcomed. Prototyping assures that system requirements are adequately defined and correct through actual user experience in using the model. Prototyping also addresses the question of timely delivery of completed systems. It is especially useful in the development of unstructured application systems.

In practice, software prototyping is done in many ways. For example, a prototyped system may be:

- Developed for a single user or multiple users.
- Programmed in one language for model development and later programmed in or combined with other language(s) to suit the operational (production) environment.
- Developed for both accounting/financial and nonfinancial systems.
- Developed to address partial or full system functions.
- Developed to build the final (real) system to operate in a production environment.

Different approaches are used to achieve the prototype variations mentioned, which is accomplished either by shortening or replacing the traditional SDLC phases. Prototyping can be viewed as the development of a **working model** with test or real (preferred) data using an iterative approach supported by user and developer interaction. Here the user is a functional user, and the developer is a data processing staff member (a programmer or systems analyst). Prototyping is done with the use of a **workbench or workstation concept** where functional user(s) and systems analyst(s) interact with the prototyping software in developing a working model. In some organizations, the information center staff assists functional users in developing prototyping models. Prototyping is meant to be a learning process in developing usable systems.

Functional users working with the system analyst or programmer/analyst use the model to experiment and understand the system/business requirements. With this approach, system fallacies can be eliminated or minimized quickly before they can get bigger. Usually models include

online terminal screens with editing functions for data input and output, flow-logic between screens, error handling rules, and batch reports. System users can define system input, process, and output functions; indicate the sequence of screens and functions; and specify data editing and validation rules to the system analyst. This method leads to an accurate data collection and processing, which improves the reliability and integrity of the system.

The system model with its inputs, processes, and outputs can be mocked up either on paper or on computer (preferred) with real data. The model is tested, changed, and retested until users are satisfied with it. With this approach, end users will get a **look-and-feel** sense of a proposed system. All changes are handled during successive iterations of the model. Later these prototyped models are either expanded in the same programming language or rewritten in another programming language to include all functions and features that are expected in a final system. Typically, the final system may use multiple programming languages, such as Assembler (a second-generation language), COBOL (a third-generation language), FOCUS (a fourth-generation language), and/or PROLOG (a fifth-generation language). Data flow diagrams and a data dictionary are some of the important tools used to document the prototype features and functions.

Often a major question is whether prototyped systems can be directly moved into production operations. The answer depends on the size, type, and nature of the system (i.e., whether it is a heavy-duty, large and complex, and transaction-based business application system; a decision-support system; a small system; a onetime system; or an ad hoc inquiry system).

Generally, heavy-duty, large and complex, and transaction-based prototyped systems should not be moved as is (directly) into production operations until full-scale design, programming, and testing activities are completed. However, for small and simple systems, onetime systems, decision-support systems, and ad hoc systems, the prototyped system and the production system could be the same.

An organization has at least three choices after a prototype is completed: (1) discard the prototype (i.e., throwaway prototype), (2) move the prototype into production operations as is, or (3) use the prototype as a starting point for the full-scale design work.

1. **Throwaway prototype.** The prototype could be discarded because it is not serving the system objectives or may be addressing wrong problems. In some cases, the model is thrown away because the system performance is so bad that it cannot be improved or the system cannot be used in multiuser environment.
2. **Use as is.** The prototype could become the actual system that can be operated in a production environment. Usually this choice is good for application systems with low-volume transactions, operated on a regular or an irregular basis. Examples are decision-support systems, ad hoc inquiry systems, onetime systems, small and simple systems, and single-user systems.
3. **Input to full-scale design.** The prototype could become the basis for a full-scale system design, programming, and testing work using the SDLC approach. Usually this choice is good for application systems with large-volume transactions, with a need for quick response time and to operate on a scheduled basis. In this case, a programming language other than the one used in developing the prototyping model may be implemented for the production environment. Under these conditions, the original prototype model could be thrown away. Examples are heavy-duty, large and complex, and transaction-based business application systems, whether accounting/financial systems or not.

(B) Cleanroom Software Engineering The primary goal of software quality assurance (SQA) is to enhance the quality of software. Cleanroom process or cleanroom software engineering is deployed to ensure software quality. With cleanroom processes, programmers do not compile their code. Instead, they spend more time on design, using a box structure method and analyzing their own work. When the programmers are confident of their work, it is submitted to another group, whose members then compile and test the code. Cleanroom experiments have shown that a lower error rate in the finished software product and an increase in productivity across a system's life cycle are possible.

Cleanroom software engineering, which is a concept borrowed from cleanroom hardware engineering, is the result of the combined effect of statistical quality control and proof-of-correctness principles. The first priority of the cleanroom process is defect prevention, not defect removal. It is understood that any defects not prevented should be removed. This priority is achieved through human verification procedures to assure proof of correctness instead of program debugging to prepare the software for system test. The next priority is to provide quality assurance, which is measured in terms of mean time to failure (MTTF). Both of these priorities eventually reflect in lowering the number of defects per thousand lines of code before the first executable tests are conducted.

(C) Computer-Aided Software Engineering Computer-aided software engineering (CASE) tools, compilers, and assemblers are used to expedite and improve the productivity of software developers' work. CASE tools provide a 4GL or application generator for fast code writing, flowcharting, data flow diagramming, data dictionary facility, and word processing in order to develop and document the new software. The CASE tools are used in prototyping the system by developing online screens and reports for the end user to view and change, as needed. Modern CASE tools are often called integrated CASE tools due to their integration of several tools.

(iv) Alternative Approaches to Develop or Acquire Software

Several alternative approaches or sources are available to organizations when planning to acquire software. Examples are listed next.

- Commercial off-the-shelf software
- Custom software
- Modifiable off-the-shelf software
- Government off-the-shelf software
- Mobile code software
- Freeware
- Shareware
- Open source software
- Embedded software
- Integrated software
- Software service from an application service provider (ASP)

Each approach is described in the paragraphs that follow

Commercial-off-the shelf (COTS) is a term for proprietary software products (including software appliances) that are ready-made and available for sale to customers.

Custom software is developed for either a specific organization or a function that differs from other already available software, such as COTS. It is generally not targeted to the mass market but is usually created for interested organizations.

Modifiable off-the-shelf (MOTS) software is typically a COTS product whose source code can be modified. The product may be customized by the purchaser, the vendor, or another party to meet customer requirements.

Government off-the shelf (GOTS) software products are typically developed by the internal IT staff of a specific government agency and can be used by other agencies. GOTS can sometimes be developed by an external contractor, but with funding and product specification from the agency.

Mobile code software modules are obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient. Mobile code is risky because it is passed from one system to another and is used to describe applets within web browsers.

Freeware is copyrighted software that is available for use free of charge for an unlimited time.

Shareware is a marketing method for commercial software, whereby a trial version is distributed in advance and without payment, as is common for proprietary software. Shareware software is typically obtained free of charge and is also known as try before you buy, demo-ware, and trial-ware. Although it is typically obtained free of charge, a payment is often required once a set period of time has elapsed after installation.

Open source software is computer software whose source code is available under a copyright license that permits users to study, change, and improve the software as well as to redistribute it in modified or unmodified form. Usually it is not obtained by a contract, but a fee may be charged for use.

There are eight possible risks from the use open source software. These include not knowing whether:

1. The software is original source or a modified version (modified software can introduce malicious code or other vulnerabilities)
2. The software infringes on any copyright or patent
3. The software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used
4. Whether the software is designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user, and system isolation)
5. The software was measured or assessed for its resistance to identified relevant attack patterns
6. The software was subjected to thorough security testing with results posted
7. Patches are distributed or whether patches can be uninstalled
8. The vendor practices version management

Embedded software is part of a lager physical system and performs some of the requirements of that system (e.g., software used in an automobile or rapid transit, traffic control, or aircraft system) and may or may not provide an interface with the user. Embedded software is internally built within the physical system.

Integrated software results from when there is a prime contractor with multiple subcontractors, as in a supply chain environment. Each subcontractor provides a specific piece of software product and/or service for the software-intensive system. The prime contractor is responsible for integrating all the pieces into a whole software-intensive system, or that contractor may hire a separate contractor to integrate it. Due to multiple contractors and subcontractors involved in supply chain environments, security risks to user organizations can increase.

If a supplier is acting as an **application service provider (ASP)** and offering to provide software as a service, instead of a stand-alone software package product, software acquirers should consider the governance of these services. Here "governance" refers to the computer programs, processes, and procedures that the ASP organization puts in place to ensure that things are done right in accordance with best practices and principles. The ASP should provide appropriate access controls, audit, monitoring, and alerting activities. Note that with the ASP, a user organization is acquiring services, not products.

When considering these alternative approaches to software, application owners and acquirers should seek to reduce or manage the risks because each alternative can introduce its own, new risks. It is highly recommended that due care principles be applied and due diligence reviews be performed to reduce such risks.

Specifically, application owners and acquires should perform these analyses to reduce risks:

- Evaluate alternatives for treatment of risks (i.e., accept, mitigate, avoid, transfer, or share with a third-party supplier).
- Identify protection strategies (i.e., security objectives and security controls) that reduce risks to levels within acceptable tolerance.
- Identify potential trade-offs among decreased risks, increased costs, and decreased operational effectiveness and efficiency.
- Identify approaches for managing residual risks that remain after protection strategies are adopted.

(v) Due Care and Due Diligence Reviews in Software Development and Acquisition

Regardless of the software alternative selected, due care and due diligence reviews are required because each software source can introduce its own risks. This is because there are many parties involved (e.g., integrators, suppliers, prime contractors, and subcontractors) in the development, maintenance, and distribution of software chain, which is a risky to manage.

Due care means reasonable care that promotes the common good. It is maintaining minimal and customary practices and/or following the best practices. Due care is the responsibility that managers and their organizations have a duty to provide for information security to ensure that the type, cost, and deployment of control are appropriate for the system being managed. Another related concept of due care is good faith, which means showing both honesty in fact and honesty in intent. Both due care and due diligence are similar to the prudent man concept.

Due diligence requires organizations to develop and implement an effective system of controls, policies, and procedures to prevent and detect violation of policies and laws. It requires that the organization has taken minimum and necessary steps in its power and authority to prevent and detect violation of policies and laws. In other words, due diligence is the care that a reasonable person exercises under the circumstances to avoid harm to other persons or to their property. Due diligence is another way of saying due care. Both due care and due diligence are similar to the prudent man concept. Note that due diligence defense is available to a defendant in a legal case in that the defendant is not liable when he or she follows all the prescribed legal procedures.

Some examples of applications of due diligence reviews are listed next.

- An information security team reviews policies, procedures, and controls during acquisition and divestiture of security-related products and services, including initial screening of vendors and suppliers, performing make-or-buy or lease-or-purchase analysis, understanding contracts, and negotiating with suppliers and contractors.
- A software acquirer requires potential software suppliers to be evaluated qualitatively and quantitatively to ensure software quality prior to contract negotiations in order to make a go/no-go decision in selecting suppliers.
- Suppliers that provide computer products and services for regulated pharmaceutical operations are audited.
- Software suppliers who claim mature process capabilities prove their software assurance practices.
- The appropriate set of security controls to adequately mitigate risk and to protect the confidentiality, integrity, and availability of data/information and information systems is selected.
- A user organization outsources media sanitization work with a contractual agreement.
- Encryption mechanisms are used for web sessions whenever a rented application requires the confidentiality of application interactions with other applications, data transfers, and data storage.

(b) Information Systems Development

This section covers applying security engineering principles; practicing defensive programming techniques; using system design principles; and implementing software assurance, safety, security, and quality techniques. These principles and techniques should be considered during information systems development to lay a strong foundation for information systems.

(i) Security Engineering Principles

(A) Purpose A principle is a rule or standard for good cause or behavior. Principles will provide a baseline for achieving security. IT security is a critical element in the system life cycle. The purpose of the engineering principles for IT security is to present a list of system-level security principles to be considered in the design, development, and operation of an information system. Ideally, the principles would be used from the onset of a program—at the beginning of or during the initiation phase—and then would be employed throughout the system's life cycle. However, these principles are also helpful in affirming and confirming the security posture of already deployed

information system. The principles are short and concise and can be used by organizations to develop their system life cycle policies.[1]

Effective information assurance rests on five system security concepts:

1. Managing, not preventing, risk
2. Acknowledging that security is a system-level attribute
3. Recognizing that changing mission or business processes results in the increased need for technical protection methods
4. Recognizing that the enterprise is made up of interrelated security domains
5. Providing security mechanisms and services to support security implementation, both domain-specific and interdomain implementation.

(B) Principle The 33 IT engineering security principles are grouped into six categories:

1. Security foundation
2. Risk based
3. Ease of use
4. Greater resilience
5. Reduce vulnerabilities
6. Use network-minded design

Category 1: Security Foundation

Principle 1. Establish a sound security policy as the foundation for design.

Principle 2. Treat security as an integral part of the overall system design.

Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.

Principle 4. Ensure that developers are trained in how to develop secure software.

Category 2: Risk Based

Principle 5. Reduce risk to an acceptable level.

Principle 6. Assume that external systems are insecure.

Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.

Principle 8. Implement tailored system security measures to meet organizational security goals.

Principle 9. Protect information while it is being processed, in transit, and in storage.

[1] Security Engineering Principles (NIST SP-800-27), U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, March 2006.

Principle 10. Consider custom-developed products to achieve adequate security. Here, "adequate security" is defined as security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Principle 11. Protect against all likely classes of attacks.

Category 3: Ease of Use

Principle 12. Where possible, base security on open standards for portability and interoperability.

Principle 13. Use a common computer language in developing security requirements.

Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

Principle 15. Strive for operational ease of use.

Category 4: Greater Resilience

Principle 16. Implement layered security to ensure no single point of vulnerability exists.

Principle 17. Design and operate an IT system to limit damage and to be resilient in response.

Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.

Principle 19. Limit or contain vulnerabilities.

Principle 20. Isolate public access systems from mission-critical resources (e.g., data and processes).

Principle 21.Use boundary mechanisms to separate computing systems and network infrastructures.

Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.

Category 5: Reduce Vulnerabilities

Principle 24. Strive for simplicity.

Principle 25. Minimize the system elements to be trusted.

Principle 26. Implement the least-privilege access principle.

Principle 27. Do not implement unnecessary security mechanisms.

Principle 28. Ensure proper security in the shutdown or disposal of a system.

Principle 29. Identify and prevent common errors and vulnerabilities.

Category 6: Use Network-Minded Design

Principle 30. Implement security through a combination of measures distributed physically and logically.

Principle 31. Formulate security measures to address multiple overlapping information domains.

Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.

Principle 33. Use unique identities to ensure individual accountability.

(ii) Defensive Programming Techniques

Defensive programming techniques include robust programming, N-version programming, fault-tolerant programming, and secure coding practices.

Robust programming makes a computer system more reliable with various programming techniques. It has five attributes:

1. It addresses interface faults during program routine invocations.
2. It practices the use of GOTO-less programming commands to minimize program complexity and errors.
3. It performs type-checking to detect human typing errors occurring during program coding.
4. It properly handles standard domains for correct inputs and exception domains for incorrect inputs.
5. It keeps the domain of unexpected exceptions, which is not caught, as small as possible because this category makes the system unreliable. The category of expected exception domain, which is caught, makes the system reliable.

N-version programming is based on design or version diversity. Different versions (i.e., ITON) of the software are developed independently. It is hoped that these versions are independent in their failure behavior. The different versions are executed in parallel, and the results are voted on.

Fault-tolerant programming is robust programming plus redundancy features and is somewhat similar to N-version programming. In summary, in fault-tolerant programming, (1) the programming language is studied to identify error-prone program constructs and to ensure that only safe program constructs are used, (2) program components are tested for faulty inputs, and (3) redundancy features are added to repair inadvertent events later.

Secure coding practices include good programming techniques with security-relevant functions. Some examples are listed next.

- Using the principles of data abstraction
- Using key attributes, such as low coupling and high cohesion, to bind modules together
- Using regression testing to verify compliance of library functions
- Using short functions and single-purpose functions
- Using single entry and single exit points in subsystems

- Minimizing interface ambiguities
- Checking for error conditions
- Encrypting important code
- Controlling the application program interfaces (APIs)
- Separating test libraries from production libraries so that the latter ones are not corrupted
- Validating inputs
- Using tools such as static code checkers, runtime code checkers, profiling tools, penetration testing tools, and application scanning tools
- Sanitizing data sent to other systems

(iii) System Design and Coding Principles

Both application systems and information systems should be designed and developed based on proven principles so systems are operated in a controlled environment. Some examples of system design principles are listed next.

The **principle of separation of privileges** asserts that protection mechanisms where two cryptographic keys or dual controls by different parties are required for access are stronger mechanisms than those requiring only one key. This principle is often implemented with access rules.

The **principle of least privilege** specifies that every program and user of the system should operate using the least set of privileges necessary to complete the job. One effect of this principle is that the potential for damage caused by an accident or an error is limited. This principle addresses the need for minimal interactions between privileged programs and the need to prevent improper uses of privilege.

The **principle of least functionality** (or minimal functionality) states that an information system's security functions should configure the system to provide only essential capabilities and specifically prohibits or restricts the use of risky (by default) and unnecessary functions, ports, protocols, and/or services. Note that the principle of least functionality facilitates the implementation of the principle of separation of privileges and the principle of least privileges.

The **principle of security by obscurity** (Kerckhoff's principle) does not work in practice because attackers can compromise the security system at any time. This principle means that trying to keep something secret when it is not does more harm than good.

The **principle of data hiding** is closely tied to modularity and abstraction and subsequently to maintainability. "Data hiding" means data and procedures in a module are hidden from other parts of the software. Errors contained in one module are restricted to that module only, not passed to other modules. Data hiding prevents components' actions from interfering with other components. Data hiding suggests developing independent modules that communicate with one another only that information necessary to achieve software function. Abstraction helps to define the procedures, while data hiding defines access restrictions to procedures and local data structures. The concept of data hiding is useful during program testing and software maintenance. Note that layering, abstraction, and data hiding are protection mechanisms in security design architecture.

The **principle of process isolation, system isolation, and component isolation** is employed to preserve the object's wholeness and subject's adherence to a code of behavior. It is necessary to prevent objects from colliding or interfering with one another and to prevent actions of active agents (subjects) from interfering or colluding with one another. Further, it is necessary to ensure that objects and active agents maintain a correspondence to one another so that (1) the actions of one agent cannot affect the states of objects to which that agent should not have correspondence and (2) the states of objects cannot affect the actions of agents to which they should not have correspondence. Isolation can exist at process, system, or component level.

Process isolation prevents data leakages and data modification problems. Techniques such as encapsulation, time multiplexing of shared resources, naming distinctions, and virtual mapping are used to employ the process isolation or separation concept. These separation concepts are supported by incorporating the principle of least privilege.

System isolation can be achieved in four ways:

1. Physical/logical isolation at the system level
2. Virtualization using virtual machines
3. Isolating tightly bounded and proprietary program components
4. Implementing standard interfaces and protocols rather than proprietary interfaces and protocols

Another related concept is component isolation, where components critical to system safety, security, and integrity are isolated from other parts of the system. Safety functions should be kept separate from one another. "Security isolation" means the information system isolates security functions from nonsecurity functions implemented via partitions and domains that control access to and protects the integrity of the hardware, software, and firmware that perform those security functions.

The **principle of fail-safe defaults** asserts that access decisions should be based on permission rather than exclusion. This equates to the condition in which lack of access is the default, and the protection scheme recognizes permissible actions rather than prohibited actions. Also, failures due to flaws in exclusion-based systems tend to grant (unauthorized) permission, whereas permission-based systems tend to fail-safe with permission denied.

The **principle of application system portioning** states that the information system should separate user functionality, including user interface services, from information system management functionality, including databases, network components, workstations, or servers. This separation is achieved through physical or logical methods using different computers, different central processing units (CPUs), different instances of the operating system, different network addresses, or a combination of these methods. Similarly, security functions should be separated from nonsecurity functions. One way to prevent access to information system management functions is to use a gray-out option for nonprivileged users, separating them from privileged users with administrator privileges.

The **principles of secure coding** include those listed next.

- Minimize the attack surface area.
- Establish secure defaults.

- Follow the principle of least privilege.
- Implement the principle of defense in depth.
- Fail securely in a known state.
- Do not trust servers.
- Implement separation of duties by separating job functions between designers and programmers, between programmers and testers, and between production staff and nonproduction staff.
- Avoid security by obscurity.
- Keep security simple.
- Fix security issues correctly.

(iv) Software Assurance, Safety, Security, and Quality

Critical software is software the failure of which could have an impact on security, safety, or privacy or could cause large financial, property, human, or social loss. It is also referred to as high-consequence software and software-intensive system. A software-intensive system is a system in which the majority of components are implemented in or by software and the functional objectives are achieved through software components.

Security controls over the critical software are listed next.

- Defensive design and programming techniques
- Robust identity and authentication methods
- Resilient/robust/trustworthy software
- Agile defenses to protect supply chain software and against advanced persistent threats using boundary protection mechanisms and information system resilience concepts
- Built-in software defenses
- Defense-in-depth strategies
- Defense-in-breadth strategies
- Defense-in-technology strategies
- Defense-in-time strategies

The scope of a secure software environment consists of software safety and software quality because security of an information system depends on both safety and quality elements of the system. An information system should have the right amounts security controls, software safety functions, and software quality features.

(A) Software Assurance Software assurance is related to reducing the level of uncertainty in software in terms of estimation, prediction, information, inference, or achievement of a specific goal. Such a reduction can provide an improved basis for justified confidence in software.

Contrast software assurance to information assurance where the latter is related to measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(B) Software Safety Software safety is important, since lack of safety considerations in a computer-based application system can cause danger or injury to people and/or damage to equipment and property. It could also create financial or other loss to people using or affected by the system. For example, an incorrectly programmed and incompletely tested medical diagnostic and treatment prescription system could kill a patient or injure people receiving the treatment. Another example is a process control system in a pharmaceutical company; drugs that are incorrectly formulated by a computer system could kill or injure patients due to errors in software. Similarly, incorrect and obsolete documentation, especially after a program change was made, could lead to improperly functioning software, loss of life, failed missions, and lost time.

Software needs to be developed using specific software development and software assurance processes to protect against or mitigate software failure. A complete software safety standard references other standards that address these processes and includes a software safety policy usually identifying required functionality to protect against or mitigate failure.

WHAT ARE THE MAJOR ATTRIBUTES OF SOFTWARE?

Polls and surveys have revealed that the top two most important attributes of software are (1) reliable software that functions as promised and (2) software free from security vulnerabilities and malicious code.

As software is included in more and more critical systems (e.g., medical devices, nuclear power plants, and transportation systems), the need for software safety programs becomes crucial. These software safety programs should consist not only of software safety analyses but methodologies that assist in the assurance of developing quality software.

Software safety should not be confused with software reliability. "Reliability" is the ability of a system to perform its required functions under stated conditions for a specified period of time. "Safety" is the probability that conditions (hazards) that can lead to a mishap do not occur, whether the intended function is performed or not. Reliability concerns all possible software errors, while safety is concerned only with those errors that cause actual system hazards. Software safety and software reliability are part of software quality. "Quality" is the degree to which a system meets specified requirements and customer or user needs or expectations.

The overall purpose of the software safety evaluation review is to assess how well the product meets its software quality objectives. Quality objectives include reliability, safety, functionality, maintainability, and reviewability. To perform this evaluation, reviewers need sufficient information about the product requirements, its development, and its overall quality.

These general types of questions can guide the reviewer regarding the product evaluation.

- How thoroughly has the developer or vendor analyzed the safety of critical functions of the software?
- How well has the developer or vendor established the appropriateness of the functions, algorithms, and knowledge on which the software is based?
- How carefully has the developer or vendor implemented the safety and performance requirements of the software?

Specific safety questions for the requirements and design phases include these six:

1. Are the safety requirements consistent with the hazard analysis?
2. How was failure analysis of the software conducted?
3. Are there requirements for self-supervision of the software?
4. Is there modularity in the design?
5. Have critical components been isolated?
6. Were design reviews performed and documented?

Specific safety questions for the implementation phase include these three:

1. Do the test cases produce results identical with the expected output?
2. Does the operations procedure manual adequately describe diagnostic procedures and tools?
3. Does the operations procedure manual adequately describe emergency procedures and fault recovery procedures?

Specific safety questions for the maintenance phase include these two:

1. Is there a formal procedure to start maintenance when problems are found?
2. Is there a formal change control procedure?

(C) Software Quality Assurance **Software quality assurance** is a planned systematic pattern for all actions necessary to provide adequate confidence that the product, or process by which the product is developed, conforms to established requirements.

The primary goal of SQA is to enhance the quality of software. The thrust of SQA is product or service assurance. Quality of process is related to the quality of product. New SQA focuses on evaluating the processes by which products are developed or manufactured.

The major objectives of the SQA process are to ensure that the software development and software assurance processes comply with software assurance plans and standards and to recommend process improvements. The process uses the system requirements and information about the purpose and criticality of the software to evaluate the outputs of the software development and software assurance processes. It begins before the software requirements process and ends when its objectives have been met. An SQA plan and review/audit reports are produced during the SQA process.

(c) Application Development

This section covers scope of application systems; responsibilities of information systems management; software testing objectives, approaches, methods, and controls; software reviews, inspections, traceability analysis, and walk-throughs; risks and threats in systems development and in systems operation; and sample audit findings in application development.

(i) Scope of Application Systems

Application-oriented information systems encompass all areas of business functions, such as manufacturing and service (operations), marketing and sales, human resources, quality, accounting,

finance, logistics, IT, and customer service. These application systems represent mission-critical systems with a strategic focus, and they are used by internal managers and executives to make decisions and by employees at all levels to perform their job duties.

EXAMPLES OF APPLICATION SYSTEMS

- General ledger
- Insurance claims processing
- Accounts payable
- Demand deposits
- Payroll
- Welfare payments
- Order entry
- Tax administration
- Sales forecasting
- License administration
- Manufacturing scheduling
- Accounts receivable

Each application system is designed to perform specific functions, similar to a manual system, with clearly defined input, processing, and output activities and boundaries. Each application system under design and development should incorporate an appropriate type and amount of application controls and security controls. Application controls are primarily concerned with data being originated, prepared, entered, processed, stored, accessed, transmitted, secured, controlled, and used. Security controls are primarily concerned with access controls, identification and authentication controls for users and applications, encryption, and password management.

(A) Data Origination, Preparation, and Input Several approaches exist to data preparation and data entry into the application system. In some cases, data are captured on a paper (source) document, such as a sales order or purchase order. The source documents are batched into small groups and entered into the system either by functional users or central data entry operators through the use of terminals. In other cases, there is no externally generated source document; instead, the customer calls in and places an order with the organization.

Regardless of the method used to capture the data, the entered data are edited and validated for preventing or detecting errors and omissions. Therefore, access controls and data editing and validation controls are important to ensure that quality data are entering into the application system.

Program-based controls are embedded in online data entry programs in the form of data editing and validation routines. These routines will ensure data integrity. The sequence of events followed by the computer center in a typical batch data entry and batch updating or online data entry and batch updating environment includes:

- Batching records of transactions or source documents.
- Converting (keying) transactions or documents to machine-readable form.

- Validating input transactions.
- Updating the master file with new transactions.
- Generating hard-copy reports.

(B) Data Processing Processing controls should satisfy these objectives:

- All transactions are authorized prior to processing.
- All approved transactions are entered quickly in their entirety and accepted by the system.
- All transactions are accurately and quickly processed.

Understanding the nature of computer processing is critical. Although there are some common controls, controls will be different between batch and online processing. Similar to data input, data editing and validation controls are important during computer processing. Therefore, more use of program-based processing controls is needed to ensure data integrity and security.

DATA PROCESSING RULES

- If an error occurs when processing a transaction, processing should be continued with that transaction. All errors and rejected transactions should be listed in a report or displayed on a computer terminal.
- When updating a batched file, and if end-of-file condition is reached on the master file before end of file is reached on the transaction file, the application program should post the remaining transactions to the master file.

The process of carrying forward control totals from one run to another is known as **run-to-run balancing**. Run-to-run control totals are program processing-based controls. Examples could be the number of records in a file and amount totals for certain data fields. The objective is to maintain the accuracy and completeness of data as they pass through computer programs and processing operations (i.e., processing control). It is good to automate the batch report balancing and reconciliation procedures and return this function to functional user departments. Functional user control of report balancing activity increases the chances of correcting the source of out-of-balance conditions. This is because the functional users have intimate knowledge have about the nature of transactions and their interrelationships. Computer operators should not perform run-to-run balancing procedures.

(C) Data Output There are many output devices in use. Some examples are terminals, printers, plotters, microfilm, microfiche, and voice response units. System output documents are photographed onto a roll of film and stored on microfilm, microfiche, and optical disk. Audio response systems will help people to inquire about a customer's bank balance, get the time and temperature readings, and obtain a telephone number from a directory. Usually system outputs are in the form of hard-copy reports. Balancing, distribution, and retention of system outputs are of major concerns to management and the auditor alike since they affect the quality and timeliness of data and usefulness of the system.

(D) Documentation System documentation is a key element of system operations. Without correct and complete documentation, new users cannot be trained properly, programmers

cannot maintain the system correctly, system users cannot make any meaningful references to the system functions and features, management or anyone else cannot understand the system functions and features, and system reviewers (e.g., auditors) cannot make objective evaluation of the system functions and controls. Application system documentation is classified into six categories:

1. System
2. Program
3. Computer operations
4. Help desk
5. Network control
6. User

This classification is based on the major user of the documentation. For example, help desk documentation is used by help desk staff.

(E) Data Integrity Integrity is binary in nature: It exists or it does not. Likewise, information quality is binary. In that it meets system user requirements or it does not. Quality is a matter of characteristics.

The perception of quality depends on the purpose for which information is to be used. For information to be useful, it should be available where, when, and in the form it is required with costs equal to or less than benefits to be derived from it.

The data have a certain degree of quality, and the user has some expectations of quality. If the data quality equals or exceeds the expectations of quality, the data have integrity; otherwise, they do not. Other factors of data quality, in addition to completeness, accuracy, and timeliness, are relevance and validity. Relevance is a measure of the appropriateness of the data item in relation to the user's problem or need. Validity is a notion of external reference or correspondence. Data may be valid but not relevant or may have low validity but still be relevant.

Data integrity is the heart of any application system. Data integrity controls ensure the reliability and usability of data and information in making management decisions. The higher the integrity of controls, the greater the credibility and reliability of application systems. Here, "data integrity" refers to five control attributes: completeness, accuracy, authorization, consistency, and timeliness.

DATA INTEGRITY RULES AND CONTROLS

- A directive control will ensure that people follow data integrity rules consistently.
- A preventive control will stop a data integrity violation from happening.
- A detective control will recognize a data integrity violation.
- A corrective control will fix or repair the damage done by a data integrity violation.
- A recovery control will help in recovering or restoring from a disaster caused by a data integrity violation.

(ii) Responsibilities of Information Systems Management

A brief list of responsibilities of information systems management in developing or acquiring systems follows. It:

- Develops, disseminates, and reviews/updates at defined frequency:
  - A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
  - Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
- Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process.
- Manages the information system using an SDLC methodology that includes information security considerations.
- Defines and documents information system security roles and responsibilities throughout the SDLC.
- Identifies individuals having information system security roles and responsibilities.
- Includes security functional requirements and specifications.
- Includes security-related documentation requirements.
- Includes developmental and evaluation-related assurance requirements.
- Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that:
  - Implements secure configuration, installation, and operation of the information system.
  - Ensures effective use and maintenance of security features or functions.
  - Understands known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
- Obtains, protects as required, and makes available to authorized personnel user documentation for the information system that:
  - Develops user-accessible security features and functions and explains how to use those security features or functions effectively.
  - Implements methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.
  - Defines user responsibilities in maintaining the security of the information and information system.
- Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
- Uses software and associated documentation in accordance with contract agreements and copyright law.
- Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.

- Controls and documents the use of peer-to-peer file-sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
- Prohibits the use of binary or machine-executable code from sources with limited or no warranty without accompanying source code.
- Enforces explicit rules governing the installation of software by users. If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect).
- Conducts due care and due diligence reviews during software development and acquisition processes.

(iii) Software Testing Objectives, Approaches, Methods, and Controls

Several testing objectives exist to test either developed or acquired information systems, and each objective may be suitable to a specific program, module, subsystem, or the entire system. In practice, compatible test objectives should be combined after considering the time, cost, and skills constraints (e.g., recovery test, security test, and configuration test). Testing is important to ensure that security-related functions and business-related functions work correctly.

Testing approaches include the big-bang, top-down, bottom-up, and sandwich approach. The big-bang testing approach puts all the units or modules together at once, with no stubs or drivers. In it, all the program units are compiled and tested at once. The top-down testing approach uses stubs. The actual code for lower-level units is replaced by a stub, which is a throwaway code that takes the place of the actual code. Bottom-up testing approach uses drivers. Units at higher levels are replaced by drivers that emulate the procedure calls. Drivers are also a form of throwaway code. Sandwich testing approach uses a combination of top-down (stubs) and bottom-up (drivers) approaches.

Several testing methods are available to test computer programs at a detailed level, each with a different focus. Specific and detailed application software testing methods with their objectives are listed next.

- **Resiliency test.** Measures durability of a system in withstanding system failures.
- **Conformance test.** Determines if a product satisfies the criteria specified in standard documents.
- **Conversion test.** Determines whether old data files and record balances are carried forward accurately, completely, and properly to the new system.
- **Interface test.** Demonstrates that all systems work in concert. (Input/output description errors are detected in the interface testing phase.)
- **Recovery test.** Determines whether the system can function normally after a system failure, error, or other malfunction and determines the ability to operate within the fallback and recovery structure.
- **Security test.** Determines whether unauthorized people can use computer resources using red team and blue team testing approaches.

- **Configuration test.** Verifies that the product can be installed and operated in different hardware and software environments without using vendor default settings.
- **Integration test.** Tests a group of programs to see that a transaction or data passes between programs. It is least understood by software developers and end users due to lack of specification documents and the variety of testing methods used. A formal change control mechanism should start after completion of an integration test.
- **Regression test.** Verifies that changes do not introduce new errors. A significant amount of testing repetition occurs by design.
- **Stress test.** Verifies boundary conditions of a program.
- **Parallel test.** Verifies test results by comparing two systems with each other.
- **Performance test.** Measures resources required (e.g., memory and disk) and to determine online system response time and batch job throughput.
- **Interoperability test.** Ensures that two or more communications products (e.g., hosts or routers) can interwork and exchange data.
- **Network security test.** Ensures that network protection devices (e.g., firewalls and intrusion detection systems) selectively block packet traffic based on application system configurations.
- **Production acceptance test.** Tests operational preparedness of a new system prior to moving from the testing to the production environment. This performed by IT production staff.
- **Pilot test.** Tests a new system in one department or division at a time until enough experience is gained prior to launching an all-out implementation throughout the organization.
- **Program unit/module test.** Tests individual programs, modules, subroutines, or subprograms to verify their functionality.
- **Systems test.** Tests the entire system to prove the validity of the software requirements definition and design specifications including its interfaces. It should include a representative sample of data for both valid and invalid conditions using test data or copies of live data, not real live data.
- **User acceptance test.** Tests software functions and features, to determine if the system meets business needs and user needs, and to see if the system was developed according to end user requirements. The end user must accept the system before moving it into the production environment. The user acceptance test is performed functional user staff.
- **Load/volume test.** Tests whether simultaneous users can overload the system.
- **Concurrency test.** Tests whether multiple users can create system deadlocks or damage each other's work.
- **Quality assurance test.** Makes sure the software product fails.
- **Function test.** Verifies that each required capability and system operation is implemented correctly.
- **End-to-end test.** Verifies that a defined set of interrelated systems, which collectively support an organizational core business area or function, interoperate as intended in an operational environment (either actual or simulated). This test is conducted extensively when an internal system exchanges data with an external system.

In addition, four broad testing methods are used:

1. Black box testing
2. Gray box testing
3. White box testing
4. Independent testing

Black box testing is a basic test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. It examines the software from the user's viewpoint and determines if the data are processed according to the specifications. It does not consider implementation details. It verifies that software functions are performed correctly and that advertised security mechanisms are tested under operational conditions. It focuses on the external behavior of a system and uses the system's functional specifications to generate test cases. It ensures that the system does what it is supposed to do and does not do what it is not supposed to do. Black box testing is also known as generalized testing or functional testing. It should be combined with white box testing for maximum benefit because neither type of testing by itself does a thorough testing job. Black box testing is functional analysis of a system.

Gray box testing is a test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. It is also known as focused testing.

White box testing is a test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. It focuses on the internal behavior of a system (program structure and logic) and uses the code itself to generate test cases. The degree of coverage is used as a measure of the completeness of the test cases and test effort. White box testing is performed at the individual component level, such as program or module, not at the entire system level. It is also known as detailed testing or logic testing. It should be combined with black box testing for maximum benefit because neither type of testing by itself does a thorough testing job. White box testing is structured testing since it focuses on structural analysis of a system. It is also called glass box testing because the tester can see the inside of a system as through a glass.

Independent testing is conducted by an independent accredited software testing organization as per the ISO/IEC 17025 standard to verify that it meets both functional requirements and SQA requirements. The testing organization can use either a white box or black box scenario depending on the need.

Testing controls bring disciple and structure to the testing process. Examples of controls to be exercised during application software testing are listed next.

- Activity logs, incident reports, and software versioning are the controls used during testing.
- There is a tendency to compress system initiation, requirements definition, design, programming, and training activities. However, for quality assurance and security reasons, the testing activities should not be compressed.
- The correct sequence of tests is unit test, integration test, system test, and acceptance test.
- The correct sequence of test tasks is prepare, execute, and delete.

(iv) Software Reviews, Inspections, Traceability Analysis, and Walk-Throughs

Reviews, inspections, traceability analysis, and walk-throughs are examples of QA and QC tools used during the SDLC to ensure a safe, secure, and quality product.

Reviews are conducted in a meeting at which the requirements, design, code, or other products of software development project are presented to the user, sponsor, or other interested parties for comment and approval, often as a prerequisite for concluding a given phase of the software development process. Reviews are more formal than walk-throughs.

Inspections are evaluation techniques in which software requirements, design, code, or other products are examined by a person or group other than the author to detect faults, violations of development standards, and other problems. The type of errors detected in inspections includes incomplete requirements errors, infeasible requirements errors, and conflicting requirements errors. Inspections are more formal than walk-throughs.

DYNAMIC ANALYSIS VERSUS STATIC ANALYSIS

An application system's functions and features can be analyzed in two ways: dynamic and static.

The most common type of **dynamic analysis** technique is testing, which involves the execution of a product and analysis of its response to sets of input data to determine its validity and to detect errors. The behavioral properties of the program are also observed. Software testing is usually conducted on individual components (e.g., subroutines and modules) as they are developed, on software subsystems when they are integrated with one another or with other system components, and on the complete system.

Inspections, code reading, and tracing are examples of **static analysis**, which is the analysis of requirements, design, code, or other items either manually or automatically, without executing the subject of the analysis to determine its lexical and syntactic properties as opposed to its behavioral properties.

Traceability analysis is the process of verifying that each specified requirement has been implemented in the design or code, that all aspects of the design or code has their basis in the specified requirements, and that testing produces results that are compatible with the specified requirements. Traceability analysis is more formal than walk-throughs.

A **walk-through** is an evaluation technique in which a designer or programmer leads one or more other members of the development team through a segment of design or code, while the other members ask questions and make comments about technique and style and identify possible errors, violations of development standards, and other problems. Walk-throughs are similar to reviews but are less formal.

(v) Risks and Threats in Systems Development and in Systems Operation

When a computer system is being developed or operated, it is subjected to several risks and threats from insiders (i.e., current and previous employees) and outsiders (i.e., hackers, adversaries, contractors, suppliers, and vendors) with different threat sources and threat objectives. These risks and threats are divided into three categories, as described next.

(A) Categories of Malware Inserted during Software Development and Maintenance Work **Malware** refers to malicious software or malicious code that is designed to deny, destroy, modify, or impede the software's logic, configuration settings, data, or program library routines. Malware

can be inserted during software's development, preparation for distribution, deployment, installation, and or update. It can be planted manually or through automated means. It can also be inserted during a system's operation. Regardless of when in the software life cycle the malware is embedded, it effectively becomes part of the software and can present substantial dangers and risks. Malware has become the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within user organizations.

There are several ways in which malware is likely to be inserted during software development or maintenance: through back door or trapdoor, time bomb, logic bomb, and software holes. This malware is introduced into a system due to unnoticed, forgotten, or neglected functions or when unnecessary functions are disregarded. It can be discovered through tabletop reviews, periodic assessments, and war-dialing, war-driving, wireless scanning, and penetration testing. Not having a source code escrow is a risk in itself.

Back doors are hidden software mechanisms used to circumvent the system's perimeter defenses and security controls, often to enable an attacker to gain unauthorized remote access to the system. A **trapdoor** is a hidden software or hardware mechanism that can be triggered to permit circumvention of system protection mechanisms. It is activated in some innocent-appearing manner (e.g., a special random key sequence at a terminal). Software developers often introduce trapdoors in their code to enable them to reenter the system and perform certain functions. Note that both back doors and trapdoors are undocumented ways of gaining access to a computer system. Both are potential security risks to user organizations as they completely circumvent perimeter defenses. The terms "back door" and "trapdoor" are used synonymously.

One frequently used back door method is inserting a malicious program that listens for system commands on a particular Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. Usually, both back doors and trapdoors are introduced through software maintenance hooks because they are special instructions in software that allow easy maintenance and additional feature development. They are not clearly defined during system access or design specification and are not documented. Maintenance hooks frequently allow entry into the code at unusual points or without the usual checks, so they are a serious security risk if they are not removed prior to live implementation.

A **time bomb** is a resident computer program that triggers an unauthorized or damaging action at a predefined time.

A **logic bomb** is a resident computer program that triggers an unauthorized or damaging action when a particular event or state in the system's operation is realized—for example, when a particular packet is received.

Software holes penetrate through lack of perimeter defenses, which is risky. A software hole can reside any of the three layers (i.e., networking, operating system, or application). Software vendors or developers should provide security mechanisms to mitigate the risks. Defending the perimeter requires installing appropriate security controls at all entry points into the network, including the Internet connection. Testing the perimeter to identify back doors and software holes requires tabletop reviews, periodic assessments, and war-dialing, war-driving, wireless-scanning, and penetration testing.

Source code escrow can be risky as it is an arrangement with a third-party (e.g., a bank) to hold the software under its custody and make it available to user organizations under unusual business circumstances. This arrangement is applicable to vendor-developed applications software packages either purchased or leased by user organizations. Usually vendors do not give the source code to user organizations for proprietary reasons; only the object is provided with the package. The vendor has the obligation to ensure that the escrowed source code is an exact copy of the production source code. The concept is similar to cryptographic key escrow.

The purpose of software escrow is to provide user organizations the ability to access the source code under unusual business circumstances, such as when the vendor is going out of business or merging with or being acquired by another organization. In the absence of an escrow arrangement, two risks are possible: User organizations cannot access the source code when needed, and applications software ceases to perform its functions or the application system cannot be recovered from a disaster. There should be a written contract for the escrow arrangement signed by the vendor and reviewed by an attorney specializing in such contracts.

(B) Categories of Malware Planted on Operational Systems There are a number of ways in which malware is likely to be planted on operational systems, including those listed next.

- Viruses
- Worms
- Easter eggs (viruses)
- Trojan horses
- Zombies
- Cross-site scripting
- Robots (Botnets)
- Rootkits
- Cookies
- Adware
- Spyware
- Active content
- Applets
- Electronic Dumpster diving
- Application program interface (API) issues
- Buffer overflow

A **virus** is a self-replicating computer program (i.e., it makes copies of itself) that runs and spreads by modifying other programs or files and distributes the copies to other files, programs, or computers. A virus is a malware program and may attach itself to and becomes part of another executable program—for example, to become a delivery mechanism for malicious code or for a DoS attack. It can replicate by attaching a copy of itself to other programs or files and can trigger an additional payload when specific conditions are met.

A number of different types of viruses, which are listed next, exist.

- Boot sector virusesinfect the master boot record of a hard drive or removable disk media (e.g., thumb drives and flash drives).
- File infector viruses attach themselves to executable programs such as word processing, spreadsheet applications, and computer games.
- Macro viruses attach themselves to application documents, such as word processing files and spreadsheets, then use the application's macro programming language to execute and propagate.
- Compiled viruses have their source code converted by a compiler program into a format that can be directly executed by the operating system.
- Interpreted viruses are composed of source code that can be executed only by a particular application or service.
- Multipartite viruses use multiple infection methods, typically to infect both files and boot sectors.
- Morphing viruses change as they propagate, thus making them extremely difficult to eradicate using conventional antivirus software tools because the virus signature is constantly changing.

Some examples of virus behaviors are listed next.

- Increase in file size
- Change in update timestamp
- Sudden increase in free space
- Numerous unexpected disk accesses
- Gradual loss of available storage space
- Unusual screen activity

To protect against viruses, install antivirus software, which is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. This software detects malicious code, prevents system infection, and removes malicious code that has infected the system. There are two drawbacks associated with antivirus software tools: (1) Virus-specific software may fail to detect viruses more recent than the software, and (2) detection software may fail to detect some viruses that are already resident in memory when the software is loaded.

A **worm** is a computer program that copies itself (i.e., self-replicating) from system to system via a network and is self-contained and self-propagating. It exploits weaknesses in the operating system or inadequate system management. Releasing a worm usually results in brief but spectacular outbreaks, shutting down entire networks. Most worms infect computers as a result of a user directly executing the worm (i.e., by clicking on it). It is unrealistic to assume that users will become cautious about executing unknown files. Countermeasures against worms include:

- Identification and authentication controls.
- Configuration review tools.

- Checksum-based change detection tools.
- Intrusion detection tools.
- Wrapper programs to filter network connections.
- Stackguarding technology to control worms.
- Firewalls to protect an organization's network from other networks.

Easter eggs are viruses and they trigger when a program code is placed in software for the amusement of its developer or users. It is a nuisance to users.

A **Trojan or Trojan horse** is a nonreplicating program that appears to be benign (i.e., looks innocent) but actually has a hidden malicious purpose. When the program is invoked, so is the undesired function whose effects may not be immediately obvious.

A **zombie** is a program that is installed on one computer system with the intent of causing it to attack other computer systems in a chainlike manner.

Cross-site scripting (XSS) is an attack technique in which an attacker subverts a valid Web site, forcing it to send malicious scripting to an unsuspecting user's browser. XSS is a delivery technique for malicious code.

A **robot (bot)** is an automated software program that executes certain commands when it receives a specific input. Bots are often the technology used to implement Trojan horses, logic bombs, back doors, and spyware.

Botnet is a term for a collection of software robots (bots), which run autonomously. A bot's originator can control the group remotely, usually through a means such as Internet relay chat and usually for nefarious purposes. A botnet can comprise a collection of cracked computers running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure. Botnets are often used to send spam e-mails, and to launch DoS phishing, and virus attacks.

A **rootkit** is a collection of files that is installed on a system to alter the standard functionality of the system in a malicious and stealthy way. It is a set of tools used by an attacker after gaining root-level access to a host computer. The rootkit conceals an attacker's activities on the host and permits the attacker to maintain root-level access to the host through covert means. Here are some examples of protection methods against botnets and rootkits:

- Use and maintain antivirus software.
- Install a firewall,
- Use strong passwords.
- Update software with patches.
- Take precautions when using e-mail and Web browsers to not trigger an infection.

Cookies are small computer files that store information for a Web site on a user's computer. This information is supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or request.

Cookies have two mandatory parameters: name and value. They have four optional parameters: expiration date, path, domain, and secure. Four types of cookies exist, including persistent, session, tracking, and encrypted cookies.

Adware is any software program intended for marketing purposes, such as to deliver and display advertising banners or pop-ups to the user's computer screen or to track the user's online usage or purchasing activity. Adware tracks a user's activity and passes it to third parties without the user's knowledge or consent. **Click fraud** is possible with adware because it involves deceptions and scam that inflate advertising bills with improper charges per click in an online advertisement on the Web.

Spyware is adware intended to violate a user's privacy. Spyware is placed on a computer to secretly gather information about the user and report it. The various types of spyware include web bugs, which are tiny graphics on a Web site that are referenced within the Hypertext Markup Language (HTML) content of a Web page or e-mail to collect information about the user viewing the HTML content, and tracking cookies, which are placed on the user's computer to track activity on different Web sites and create a detailed profile of the user's behavior. To protect against spyware, install antispyware software, which is a program that specializes in detecting both malware and nonmalware forms of spyware.

Active content technologies allow code, often in the form of a script, macro, or other mobile code representation, to execute when the document is rendered. HTML and other related markup-language documents, whether delivered via HTTP or another means, provide rich mechanisms for conveying executable content. Examples of active content include Postscript and PDF documents, Web pages containing Java applets and JavaScript instructions, word processor files containing macros, spreadsheet formulas, and other interpretable content. Active content may also be distributed embedded in e-mail or as executable mail attachments. Countermeasures against active content documents include security policy, application settings, automated filters, software version control, software readers, and system isolation.

Applets are small computer applications written in various programming languages that are automatically downloaded and executed by applet-enabled Internet browsers. Examples include Active-X and Java applets, both of which have security concerns.

Electronic dumpster diving involves scanning and enumerating systems and ports to discover passwords and to investigate open-source intelligence using DNS lookups and Web searches to discover the characteristics of the system being attacked and particularly to pinpoint any potentially exploitable vulnerabilities.

API issues include calls, subroutines, or software interrupts that comprise a documented interface so that a higher-level program, such as an application program, can make use of the lower-level services and functions of another application, operating system, network operating system, or a driver. APIs can be used to write a file in an application program's proprietary format, communicate over a TCP/IP network, access a structured query language (SQL) database, or surf the Internet, which can be risky because APIs can cause buffer overflow exploits, which, in turn, lead to worm attacks.

Buffer overflow is a condition likely to occur in APIs in which more input is placed into a buffer or data-holding area than the capacity allocated, thus overwriting the information. Attackers and adversaries can exploit such a condition to crash a system or to insert

specially crafted code that allows them to gain control of the system. Some countermeasure are listed next.

- Use appropriate security controls across operational, network, and host layers, combined with applying updated antivirus software and patches.
- Installing firewalls.
- Practice secure programming techniques.
- Install intrusion detection system software.
- Use APIs with stackguarding technology.
- Monitor with security event management tools.

In addition, use Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP) instead of regular File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), as shown next.

FTP/TFTP → SFTP/SCP

(C) Categories of Nonmalware Deployed on Operational Systems Sometimes malware is combined with nonmalware deceptive practices, such as social engineering techniques, to accomplish complex attacks on unsuspecting users. Three major categories of social engineering attacks include spamming, phishing, and pharming.

Social engineering attacks occur in many ways when malware is combined with deceptive social engineering techniques to accomplish complex attacks on unsuspecting users. In some cases, deception is used to trick the user into downloading and executing malicious code. Phishing is also a deception technique, although it does not require malicious code. In other cases, malware is used to enable a deception, as in pharming. Both phishing and pharming are different forms of social engineering.

Spamming is the abuse of an e-mail system in the form of sending unsolicited bulk e-mails and junk e-mails. Recipients who click links in spam messages can inadvertently download spyware, viruses, and other malware. To protect against spamming, install a spam filtering software, which is a computer program that analyzes e-mail to look for characteristics of a spam and typically places the messages that appear to be spam in a separate e-mail folder.

Phishing is the creation and use of fraudulent but legitimately looking e-mails and Web sites to obtain Internet users' identity, authentication, or financial information or to trick users into doing something they would not do. In many cases, the perpetrators embed the illegitimate Web site's universal resource locators (URLs) in spam, in hoping that a curious recipient will click on those links and trigger the download of the malware or initiate the phishing attack.

Pharming is the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate Web site for the purpose of obtaining private information. Pharming often uses Trojan horses, worms, or virus technologies to attack the Internet browser's address bar so that the valid URL typed by the user is modified to that of the illegitimate Web site. Pharming may also exploit the DNS server by causing it to transform the legitimate host name into the invalid Web site's IP address; this form of pharming is also known as DNS cache poisoning.

(vi) Sample Audit Findings in Application Development

Sample audit findings describing what can go wrong during application systems development process are listed next. These findings are not exhaustive and are shown here just to give the reader an idea of what findings might be.

- **Audit Finding No. 1.** Internal audit was asked to help implement a new customer information system by ensuring that conversion programs were functioning properly. The auditors wrote and ran programs that matched the old and new files and printed exceptions. Several conversion program errors were discovered and corrected. As a result of the audit work, greater reliance was placed on the conversion programs, and implementation time was reduced by four person-weeks.
- **Audit Finding No. 2.** During a review of the customer information system file maintenance area, auditors noted that the only documentation for the control programs consisted of the programs themselves, which were quite complicated. It was suggested to the information system department that a statement describing these control programs would not only be excellent documentation but would provide a training tool for computer programmers. In addition, a copy of the test file, developed by the IT audit staff, was turned over to the information systems department to use in conducting independent tests of the system.
- **Audit Finding No. 3.** During an audit of a vendor-supplied and remote online computer system, the auditor noted that the contract specified that user access to the computer system was guaranteed for a total number of hours per day. The auditor pointed out that this would be meaningless because the contract failed to include any performance standards, such as maximum acceptable terminal response times or the number of file accesses necessary to ensure that the required volume of work could be processed in the designated number of hours. As a result of the auditor's recommendations, tough performance standards for the vendor to meet were included in the new contract. Failure to meet the standards would result in heavy monetary penalties for the vendor, creating a great incentive to provide acceptable service.
- **Audit Finding No. 4.** A company's sales incentive plan is complicated by the many incentive earnings determinants based on product type, product profitability, and sales volume. Incentive penalties are also provided. Using a computer program greatly facilitates the calculation of each salesperson's incentive earnings. The IT auditors employed an audit retrieval program to test the accuracy of computer calculations under various conditions. The auditors found that in the process of amending the program, the company's programmers had inadvertently changed the program so that incentive penalties were no longer calculated and charged to salespeople. Overpayments to salespeople totaling significant amounts were recovered, and procedures were strengthened to guard against unauthorized and/or improper changes in financially sensitive computer programs.

(d) Change Management and Control

Change management (CM) configuration control, access controls over changes, check-in and check-out procedures, system stages, and application software maintenance controls are presented in this section.

(i) Change Management

A formal change management program should be established and procedures should be used to ensure that all modifications to a computer system or network meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plan. The change control procedures for a software-intensive system

should ensure that software assurance requirements are not compromised when changes are requested. Each change control request should include a specific section that addresses the impact of the requested change on software assurance requirements.

Risk assessment should be performed on all changes to the system or network that could affect security, including configuration changes, the addition of network components, and installation of software. Changes to policies and procedures may also be required. The current network configuration must always be known and documented.

For example, in object-oriented database management (OODBM) system model, version management is a facility for tracking and recording changes made to data over time through the history of design changes. The version management system tracks version successors and predecessors. When objects constituting a portion of the design are retrieved, the system must ensure that versions of these objects are consistent and compatible.

WHAT IS THE DIFFERENCE BETWEEN VERSION CONTROL AND VERSION MANAGEMENT?

- **Version control** involves controlling the different versions of software, uniquely identifying versions and configurations, and providing version change history to ensure stability, traceability, and repeatability.
- A **version management system** tracks version successors and predecessors.
- Both version control and version management ensure that all versions are consistent and compatible with each other.

(ii) Configuration Management

The three essential features of CM include stability, traceability, and repeatability.

- **Stability** means that an information system will not crash, shut down, or fail. Even if it fails, it fails in a known secure state.
- **Traceability** means that one can follow the change activities from origin to destination and in between.
- **Repeatability** is the ability to reproduce any version of the software at any given time.

The correct sequence of CM activities is item identification, change control, item status accounting, and audit.

- **Configuration item (CI) identification.** A methodology for selection and naming of CIs that need to be placed under CM.
- **Configuration change control.** A process for managing updates to the baselines for the CIs.
- **CI status accounting.** Consists of recording and reporting of information needed to manage a configuration effectively.
- **Configuration audit.** Consists of periodically performing a review to ensure that the CM practices and procedures are rigorously followed. CM answers the two questions: What constitutes a software product at any point in time? and What changes have been made to the software product?

(iii) Configuration Control

Configuration control is the process of controlling modifications to hardware, firmware, and software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. Change control is related to configuration control.

The information security management:

- Determines the types of changes to the information system that are configuration controlled.
- Approves configuration-controlled changes to the system with explicit consideration of security impact analyses.
- Documents approved configuration-controlled changes to the system.
- Retains and reviews records of configuration-controlled changes to the system.
- Audits activities associated with configuration-controlled changes to the system.
- Coordinates and provides oversight for configuration change control activities through a committee or board.

Information security management and functional management determine the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to information system components, changes to the configuration settings for IT products (e.g., operating systems, applications, firewalls, and routers), emergency changes, and changes to remediate flaws.

A typical process for managing configuration changes to the information system include, for example, a chartered **configuration control board** that approves proposed changes to the system. The board is a group of qualified individuals with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operation life cycle phases of an information system. The term "auditing of changes" refers to changes in activity before and after a change is made to the system and the auditing activities required to implement the change. It is important for an information security representative to be a member of the board.

Information security management employs automated mechanisms to:

- Document proposed changes to the information system.
- Notify designated approval authorities.
- Highlight approvals that have not been received by certain date.
- Inhibit change until designated approvals are received.
- Document completed changes to the information system.

Functional management conducts tests, validates, and documents changes to the information system before implementing the changes on the operational system. Functional management ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures; the information system security policies and procedures; and the specific health, safety, and

environmental risks associated with a particular facility and/or process. An operational system may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing).

The IT software development management and the information security management employ automated mechanisms to implement changes to the current information system baseline and deploy the updated baseline across the installed base.

(iv) Access Controls over Changes

The information security management defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries.

Examples of access restrictions include, for example:

- Physical and logical access controls.
- Workflow automation.
- Media libraries.
- Abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component).
- Change windows (e.g., changes occur only during specified times and making unauthorized changes outside the change window for easy discovery).
- Authorizations to make changes to the information system.
- Auditing changes.
- Retaining and review records of changes.

Specific access controls over changes include those listed next.

- Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
- Conduct audits of information system changes at defined frequencies and when indications warrant, whether unauthorized changes have occurred or not.
- Prevent the installation of critical software programs and/or modules (e.g., patches, service packs, and device drivers) that are not signed with a certificate that is recognized and approved by the organization.

- Limit information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment.
- Review and reevaluate information system developer/integrator privileges at defined frequencies.
- Limit privileges to change software resident within software libraries, including privileged programs.
- Implement automated safeguards if security functions or mechanisms are changed inappropriately.

The information system reacts automatically when inappropriate and/or unauthorized modifications have occurred to security functions or mechanisms. Automatic implementation of safeguards and countermeasures includes, for example, reversing the change, halting the information system, or triggering an audit alert when an unauthorized modification to a critical security file occurs.

(v) Check-In and Check-Out Procedures

Check-in and check-out procedures, as they relate to a CI, are expressed in terms of a state-transition diagram that deals with events, transitions, and actions. System requirements and analysis are the major emphasis in processing a request for change. These events and actions (i.e., initial, check-out, modify, and check-in) take place when the CIs are checked in and out:

- **Initial.** The initial state assumes that the CI is checked into the CM workspace and locked without a flag.
- **Check-out.** The action here is to copy the CI to the software developer's workspace in the unlocked state. The CI is flagged as out and locked.
- **Modify.** The action is to modify the contents of the developer's workspace.
- **Check-in.** The action is to copy the modified CI to the CM workspace, remove the flag in the CM workspace, and delete the CI from the developer's workspace.

(vi) System Stages

Whether a system is database or nondatabase, a new system should go through four stages during its development: development, testing, staging (quality assurance), and production libraries. All these stages require the same security controls, especially the staging library, because that library is often copied into production library. Nonproduction environments pose a security risk due to the use of production data without masking. Therefore, nonproduction environments should be treated with the same care as the production environment. The sequence of stages is:

$$\text{Development} \rightarrow \text{Testing} \rightarrow \text{Staging} \rightarrow \text{Production}$$

(vii) Application Software Maintenance Controls

The scope of application software maintenance controls includes controls used to monitor the installation of and updates to application software to ensure that the software functions as expected and that a historical record is maintained of application system changes. Such controls also help to ensure that only authorized software is allowed on the system. These controls may include a software configuration policy that grants managerial approval to modification and then documents the changes. They may also include some products used for virus protection.

(e) End User Computing

Scope audit challenges, and audit and control risks, including suggested controls, are discussed in this section.

(i) Scope

The scope of end user computing (EUC) can be limited or extended; "limited" means that end user systems are developed to automate an individual's day-to-day work functions using small computer programs or spreadsheet applications, which is a low risk. But the risk is high with extended systems when these end user systems are uploading or downloading end user data files back and forth to LAN systems or mainframe computer systems in order to exchange and share data between these systems.

This is because end user systems, by definition, often have inadequate and incomplete application-based controls and lack effective security controls, thus compromising data integrity in all connected systems. Usually, end users deploy PCs and/or desktop computers to facilitate their work and seek help through help desk staff and IT technical support staff.

The ideal EUC system is a system that is well confined to its scope and contained within its boundary. When this is not possible, end users should obtain design and development assistance either from internal IT staff or external contractors.

(ii) Audit Challenges

According to the Institute of Internal Auditors' study results, there are seven audit challenges in EUC. Organizations and auditors must:

1. Understand the current use or impact of EUC.
2. Need to link EUC activities with business objectives.
3. Coordinate potentially synergistic EUC activities.
4. Ensure connectivity and interoperability.
5. Assist end user department managers and staff to identify business risks, control points, and benefits for adopting application-based controls and security controls.
6. Implement the application selection and development methodologies.
7. Expand audit programs to include EUC when significant financial or operational issues exist.[2]

(iii) Audit and Control Risks

A list of audit and control risks in end user–developed systems is presented next.

- Information (audit) trails, controls, and security features may not be available in the end user–developed application systems.
- Data storage and file retention, backup, purging, archiving, and rotating procedures may not be available or adequate.

[2] Larry Rittenberg and Ann Se, The IIA study on end user computing (EUC) identified seven challenges to organizations. Martin Bariff, *Audit and Control of End User Computing* (Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 1990).

- Documentation may not be available, or it is inadequate or incorrect.
- Backup and recovery procedures may not be available or effective in the application systems developed by end users.
- Program change controls may not be available or effective.

(iv) Suggested Controls

Lack of adequate separation of duties is a potential control weakness in end user systems. Direct supervision, training, and frequent work reviews should be conducted to balance the control weaknesses.

When uploading data from a personal computer (PC) to a host computer, the data conversion programs residing on the host computer should reject inaccurate or incomplete data before updating any host-resident data files. Control totals should be developed between the PC and the host computer and reconciled automatically by the program. Uploading files is one source of computer viruses, and its effects on other programs and data files are unknown.

Exhibit 6.7 presents a summary of preventive, detective, and recovery controls as they relate to PCs and EUC. Implementation of these controls would help IT management and end user management in strengthening overall controls.

Preventive controls	Detective controls	Corrective controls
Establish a PC support function	Install physical security devices	Develop control reports
Issue policies, procedures, and standards	Implement logical security mechanisms	Develop audit trail reports
Establish controls in application programs used for mini- and midrange computers (e.g., label checking, recovery procedures, batch and file balancing, audit trails)	Test end user–developed software	Develop exception reports
Require a user ID and a password prior to accessing the PC system		Develop error reports
Initiate a preventive maintenance program for the PCs		Develop activity aging reports
Install program change controls for end user–developed systems		
Require documentation for end user–developed and maintained systems		

EXHIBIT 6.7 Preventive, Detective, and Corrective Controls for PCs and End User computing

(f) Knowledge-Based Systems

The scope of knowledge-based systems includes artificial intelligence technology, parsers, neural network systems, and expert systems.

(i) Artificial Intelligence Technology

Artificial intelligence (AI) includes many disciplines, such as operations research and expert system technology. AI involves the creation of computer software that emulates the way humans

solve problems. Fifth-generation programming languages, such as PROLOG and LISP, are used in developing computer systems based on AI technology. AI is the enabling technology for parsers, neural networks, expert systems, knowledge bases, object formation, and intelligent editors. The objective of AI is to get the computer to think like a person.

(ii) Parsers

Parsing is the procedure of breaking the program code, comments, or sentences into logical parts and then explaining the form, function, and interaction of these parts. Parsers (either self-generated or user-loaded) recognize syntactic and semantic constructs in the source code and load them as object-oriented representations into a repository.

(iii) Neural Network Systems

Neural networks are AI systems built around concepts similar to the way the human brain's web of neural connections—known as synapses—is believed to work to identify patterns, learn, and reach conclusions.

Neural networks have the ability to learn and to utilize accumulated experience to make decisions that rival those of human beings. Neural networks have nothing to do with telecommunications-related networks.

Neural network systems are particularly apt for risk management and forecasting activities, in which the ability to identify intricate patterns is crucial to making predictions. In theory, a neural network can be put to work in any application in which substantial amounts of data are used to predict an outcome.

Neural networks have been used to:

- Trade securities and options.
- Identify fraudulent use of credit cards.
- Decide whether to approve a mortgage application.

A neural network develops the ability to decide and then learns to improve its performance through massive trial-and-error decision making. A neural network is trained by being supplied with key data from a sample group of transactions. The network is able to use fuzzy or incomplete data successfully and to discover patterns in decision making that conventional rule-based systems would not pick up.

(iv) Expert Systems

Expert systems (also known as knowledge-based systems) use AI programming languages to help human beings make better decisions. In the business world, managers at all levels make decisions based on incomplete data and ambiguous information and under uncertain conditions. Expert systems are built by a knowledge system builder, a knowledge engineer, a human expert in the subject matter based on rules of thumb, facts, and an expert's advice. The knowledge system builder is like a programmer, and the knowledge engineer is similar to a systems analyst in a conventional systems development environment. The human expert is a person knowledgeable in the subject matter located either inside the organization or outside. More than one expert can participate in an expert system project to develop the knowledge base.

DIFFERENCE BETWEEN CONVENTIONAL SYSTEMS AND EXPERT SYSTEMS

- Conventional systems are aimed at problems that can be solved using a purely algorithmic approach but can be solved using an SDLC methodology.
- Expert systems are aimed at problems that cannot be solved using a purely algorithmic approach but can be solved using a heuristic methodology.

Expert systems have an inference engine, which decides how to execute an application or how the rules are fired. The inference methods include forward and backward chaining (or reasoning). In forward chaining, data are subjected to rules to achieve system goals, whereas in backward chaining, the system starts with goals and works backward through the rules to determine what data are required. Facts (data) and rules are stored in the knowledge base of the system and are used in the question-and-answer session with the end user. The system can be designed with a multiple-choice question format with a list of alternatives provided, and the end user chooses one. In a way, the expert system becomes a personal consultant or guide to the end user in solving problems.

SAFETY AND SECURITY RISKS IN EXPERT SYSTEMS

- If the rules in the expert systems are not formulated properly and tested correctly, the outcomes could lead to loss of life or damage to property in medical and military systems.
- Use of too many rules in expert systems can complicate the programming work and access control decisions, thus compromising the system's security.

The operation of an expert system can be viewed in terms of the interaction of distinct components, such as the knowledge base, inference engine, and end user interface. The **knowledge base** stores knowledge about how to solve problems. Inference procedures are executed by a software module called the **inference engine**. If the user of the expert system is a person, communications with the end user are handled via an **end user interface**.

6.3 System Infrastructure

(a) Information Technology Control Frameworks

IT control frameworks provide overall guidance to user organizations as a frame of reference for security, governance, and implementation of security-related controls. Several organizations within and outside the United States provide such guidance.

Eleven major types of IT control frameworks are discussed in this section:

1. The Institute of Internal Auditors' Electronic Systems Assurance and Control (eSAC)
2. The IT Governance Institute's (ITGI's) Control Objectives for Information and Related Technology (COBIT)
3. The Information Systems Audit and Control Foundation's (ISACF's) Control Objectives for Net Centric Technology (CONCT)

4. The SysTrust Principles and Criteria for Systems Reliability from the American Institute of Certified Public Accountants/Canadian Institute of Certified Accountants (AICPA/CICA)
5. The International Federation of Accountants' (IFAC's) Managing Security of Information
6. The Information Security Forum's (ISF's) standard
7. U.S Department of Homeland Security
8. The European Union's (EU's) security directives
9. The Organisation for Economic Co-operation and Development's (OECD's) Guidelines for the Security of Information Systems
10. International Common Criteria (CC)
11. The International Organization for Standardization (ISO) standards

In addition, guidelines for implementing minimum security requirements, regardless of the type of IT control framework adopted, are presented.

(i) IIA's Electronic Systems Assurance and Control

eSAC sets the stage for effective technology and risk management by providing a framework for evaluating the e-business control environment. Within the context of an organization's mission, values, objectives, and strategies, the different eSAC modules will assist in gaining an objective perspective on the organization's IT culture. This knowledge will then aid in providing assurance to customers, regulators, management, and boards that IT risks are understood and managed.

eSAC brings executive management, corporate governance entities, and auditors new information to understand, monitor, assess, and mitigate IT risks. It will examine and assess risks that accompany each organizational component, including customers, competitors, regulators, community at large, and owners and investors. The eSAC title is enhanced by changing "Auditability" to "Assurance" to recognize the important perspectives of governance and the alliances—both within an organization and between business partners—needed to ensure effective security, auditability, and control of information.

(A) Technology Challenge of Components The technology challenge of components include open systems, technology complexity, information security, privacy concerns, and development and distribution processes.

Open Systems Internet-based distributed systems have very different characteristics from internally focused, closed private computer information systems. Open systems that use the Internet are the first truly pubic systems and as such are exposed to more and different risks. Never before have organizations been so accessible to so many. The Internet (the World Wide Web, or Web) is a global client/server environment that evolved due to low-cost powerful computers with large storage capacity, mass communications, and user-friendly software.

Technology Complexity Dispersion of technology into every department, division, or business unit provides new challenges to control and assurance. Over both proprietary and Internet connections, organizational system boundaries will blur into those of allies, partners, suppliers, and end users. Such widespread distribution will challenge already inadequate abilities to provide security, control, and privacy.

Control migration from application code to the environment is a growing trend. Traditional applications—accounting, purchasing, scheduling, manufacturing, inventory, sales, delivery, and collection—are often integrated into enterprise resource planning (ERP) systems. Data reside in one central database, with more responsibility for control. The human resources (HR) system and its database may support all employee-related activities, such as payroll, evaluations, training and skills, benefits, and retirement benefits. The ERP systems integrate traditional applications, databases, and HR systems.

The proliferation of computers and the Internet has brought technology services into even the smallest of businesses and organizations. Common applications offer enormous economies of scale, and even niche applications can thrive. Software size and complexity has consumed new capability faster than computer chips can make it available. As more people acquire computers and access spreads to more countries, the current Web will expand to even more products, services, and languages, challenging controls over users' interaction while providing the information and services they seek.

Information Security Effective security is not only a technology problem, it is a business issue. It must address people's awareness and actions, training, and especially the corporate culture, influenced by management's security consciousness and the tone at the top.

Access to computer system is not an issue; rather the issue is how much access is enough. When access exists, there is the potential for inappropriate access, introduction of errors, possible disclosure, corruption, and destruction of information. Since security is a moving target, there must be a continual risk assessment and management process to examine changing vulnerabilities and consequences and to prioritize risks and probabilities. This focuses security resources on things that must be protected and threats that can be mitigated at appropriate cost based on a cost/benefit analysis.

Privacy Concerns Countries treat privacy matters differently based on their cultures, treaties, and practices. Globalization of business due to the Internet has meant many new laws and regulations to address concerns over specific rights to control personal information. Privacy provisions range from confidentiality of communications to specific access rights. The global privacy landscape involves legislative, regulatory, and cultural considerations of overlapping or conflicting requirements that range from generally acceptable use to more restrictions in certain countries.

Development and Distribution of Processes The design and development process has changed. Formerly, systems were developed to facilitate existing business operations, but today they are frequently seen as a new line of business. E-business and the need to get to market faster often mean expansion of the IT infrastructure outside the organization. Hardware and software, telecommunications, and Web hosting are often outsourced to Internet service providers (ISPs). The provision of controls, and assurance that controls are deserving of reliance placed on them, grows exponentially more complex as the number of parties and layers grows.

Responses to the Technology Challenge Risk assessment, internal control, and e-assurance are suggested as responses to the technology challenge.

Risk Assessment Functional and technology managers must reject the silo attitude or inept behavior toward risks. An organization may do its strategic planning too quickly or not at all; it may not align strategy and enterprise design with market requirements; managers may not look beyond strict areas of their authority; compensating controls may not be designed to mitigate

local risks; or teamwork among cross functions may not exist to communicate the nature and severity of risks to senior management.

There is no standard way to measure risks and associated losses since e-commerce risks affect businesses differently. Therefore, each business unit should conduct its own risk assessment, addressing such questions as:

- What are the risks?
- How large is the adverse effect of an exposure?
- Are preventive, detective, and corrective controls in place, and are they effective?
- How much security protection against risks is justified?
- Which risks threaten survivability of the business?
- Which risks can be mitigated at relatively low cost?

Internal Control Internal control comprises the activities an organization uses to reduce risks that can affect its mission. The tone at the top (senior management) determines the focus for the entire organization, including the system of internal control. Management has direct responsibility for control and must coordinate efforts to achieve objectives. Although changes in technology present new risks and require different control techniques, basic control objectives remain essentially unchanged.

While definitions of internal control vary, they address the same objectives. The system of internal control is processes and procedures to provide reasonable assurance that goals and objectives are achieved and to ensure that risk is reduced to an acceptable level.

A cost/benefit analysis should decide which controls—internal or external—mitigate the risks most effectively. To devise an IT risk strategy, management must decide which risks are serious, which can be insured, which controls can be relied on, and which risks require compensating controls. Monitoring for compliance and constant update are essential.

E-assurance Systems are imperfect, things go wrong, and people seek assurance that prudent controls minimize risk. Assurance services check the degree to which a system deviates from industry standards or management requirements for reliability. Whenever one party makes an assertion that requires review before others can rely on it, there must be an agreed-on set of criteria against which to measure it and a process to collect such evidence. When there are few agreed-on standards, attaining such a goal becomes difficult at best.

Traditional assurance services are being revamped to meet the new challenges. The problem is the ever-shifting nature of risks and controls. As a body of data is developed, these services, along with improvements in firewalls and intelligence being built into routers, third-party certifications, trusted certificate authorities, digital signatures, and encryption using PKI and the like will combine to improve controls over e-business.

An issue exists as to whether the marketplace—internal or external—will accept that internally provided assurance by internal auditors is effective in enhancing trust. The visible trust marks and Web site seals that external assurance service providers can provide are increasingly seen as viable methods to reassure the users of e-business services. For most organizations, an appropriate balance between using internal and external assurance is the best path.

(B) eSAC Model The eSAC model's assurance objectives or control attributes, such as availability, capability, functionality, protectability, and accountability, are integrated with the the objectives of the Committee of Sponsoring Organizations (COSO), such as effectiveness and efficiency of operations, financial and other management reporting, compliance with laws and regulations, and safeguarding of assets. Privacy concerns are discussed under protectability and accountability. Next, we discuss the five assurance objectives of the eSAC model:

1. Availability
2. Capability
3. Functionality
4. Protectability
5. Accountability

Availability Information, processes, and services must be available when needed. Specifically, the organization must be able to receive, accept, process, and support transactions in a manner acceptable to its customers. Access via the Internet can mean 24/7/365 availability. To ensure availability, the auditor evaluates controls that deal with potential causes of business interruption. These might include:

- Physical and logical security of system resources.
- Mechanical failure of computer file storage devices.
- Malfunction of software or unexpected incompatibilities.
- Inadequate computer capacity planning.

In the event of a problem, controls must provide for swift recovery to the normal position.

Capability "Capability" means end-to-end reliable and timely completion and fulfillment of all transactions. This means that the system has adequate capacity, communications, and other aspects to consistently meet needs even at peak demand. For systems to provide such services, monitoring of usage, service-level agreements (SLAs) with ISPs, application service providers (ASPs), and others are important controls. It is critical that system and process bottlenecks be identified and eliminated or carefully managed—the goal is to achieve and maintain an efficient and effective balance across the organization.

Efficiency of systems is an aspect of capability that leads to effective use of resources. A key is controlling system development and acquisition methodologies to prevent cost overruns and systems that do not perform as required. To help ensure efficiency of IT, the auditor evaluates controls that deal with causes and risks of excessive costs, characterized as waste and inefficiency. Some of the problems might include:

- Weaknesses in controls that result in excessive correction of errors; prevention is usually more efficient.
- Controls that consume more resources than the benefits they deliver.

Systems that are inefficient may foster user creation of shadow systems that work around the official system. Such duplicate costs are clearly inefficient. The unreliable system must be fixed

before the shadow system is halted. The objectives of system development controls are to avoid such issues. Methodologies should result in efficient and appropriate design and development of an application and ensure that controls, auditability, and security are built into the system.

An information system that is not maintained effectively becomes unreliable. Controls over system maintenance, often called change controls, provide continuity while hardware or software changes are made and ensure that all changes are documented, approved, and confirmed. System maintenance controls include:

- Adequate user involvement in requesting, testing, and approving program changes.
- Creating appropriate audit trails, including program change history logs.
- IT and user personnel approval.
- Sufficient documentation of program changes.

Once the above controls are complete, controlled production transfer procedures reduce the risk of programmers having the ability to introduce unapproved test versions of programs into production environment.

Functionality "Functionality" means the system provides the facilities, responsiveness, and ease of use to meet user needs. Good functionality goes well beyond the minimum transaction processing. It should also provide for recording control information and other issues of concern to management. Preventing problems in functionality includes considering the perspective of untrained, possibly unknown online users. Users can become impatient and may quit without completing a transaction or may resubmit input, causing duplicates. To help ensure functionality, the auditor evaluates controls that monitor and provide feedback. Some of these might include:

- The display of progress indicators following input.
- Positive confirmation of transactions.
- Monitoring user abandonment of transactions.
- Monitoring system hangups.

Effective information is information that is relevant to the business process, delivered by a functional system. Relevance of information is based on system design, which requires user and management participation to reach functionality. Problems often stem from inadequate specifications due to lack of user involvement in system development, which usually means the resulting application will be ineffective.

To help ensure effectiveness, the auditor evaluates controls over timely, correct, consistent, and usable information. The system should permit flexible displays and reports that can be tailored to different audiences. The format in which information is delivered can have a substantial impact on how effective the communication is.

Protectability Protectability includes protection of hardware, software, and data from unauthorized access, use, or harm. Robust security is difficult to maintain due to the vast access possible via the Internet, which structure has inherent weaknesses. Controls are needed to safeguard IT assets against loss and to identify when such loss has occurred. Many current controls focus on

reducing risks of catastrophic damage, internal fraud, or embezzlement. To ensure protectability, the auditor evaluates general controls over IT that are often grouped as follows:

- **Data security and confidentiality.** Access to data, an important asset, should be limited to those authorized to process or maintain specific data or records. Protecting organizational data is the key responsibility of the information security function and its administrators. The security functions may include restricting access to data through various logical access paths, based on user requirements; restricting access to program libraries and data files on a need-to-know basis; and providing the ability to hold users accountable for activities performed.
- **Program security.** Access to program files and libraries should be restricted to authorized personnel through the use of access control and other security software. Program updates should be monitored and controlled using library management software. Appropriate segregation of duties should ensure that the programming function does not have unrestricted access to production programs.
- **Physical security.** Access to computer processors and storage devices should be limited to those (e.g., data center management and computer operations staff) requiring access to perform job functions. Access to the host server computer room should be monitored and controlled (e.g., card access control systems). Physical control over reports containing confidential data should be implemented (e.g., report distribution procedures). Physical safeguards include fire prevention, preventive maintenance, backup of data files, and property insurance.

Many protectability objectives are designed to ensure that data retains their integrity. In other words, that data are complete, accurate, and up to date and cannot be changed on an unauthorized basis. To help ensure integrity, the auditor evaluates controls over causes of erroneous data, which often are known as application controls, plus by general controls over access. More detailed integrity control objectives are listed next.

- Authorized transactions are initially and completely recorded.
- All transactions are completely and accurately entered into the system for processing.
- Approved transactions entered are accepted by the system and processed to completion.
- All transactions are processed only once; no duplicate transactions are processed.
- All transactions are processed accurately, updating the correct files and records.

Procedures should minimize the opportunity for application programmers and users to make unauthorized changes to production programs. Access to system software should be controlled to avoid direct compromise of the integrity of program code, data on file, or results of processing.

Confidentiality and privacy are issues of accountability in compliance, and protectability in making it possible. There is no privacy without security. Confidentiality refers to intellectual property, trade secrets, and strategic plans. Privacy is usually viewed in the context of personal information, including customers, employees, and stockholders, but not corporate entities.

Accountability Accountability identifies individual roles, actions, and responsibilities. It includes the concepts of data ownership, identification, and authentication, all fundamental to being able to identify who or what caused a transaction. The audit or transaction trail should have enough information—and be retained long enough—for transactions to be confirmed, if necessary.

Accountability also includes the concept of nonrepudiation. This means that once authenticated, a user cannot disclaim a transaction, as might happen when an online brokerage user seeks to break a trade that turned out to be a bad idea that he or she nonetheless actually caused.

Accountability also includes issues in granting traceable access to restricted information and software functions. This is a particular problem in IT, where systems analysts, programmers, system administrators, and the like resist controls over their own activities. In some cases, monitoring of such use, while seemingly appropriate, can be turned off by the very system administrator it is designed to watch.

Organizations need to authenticate the identity of people entrusted with authority to change data files or software. Similarly, an organization holding private information has an obligation to authenticate the identity of inquiries before disclosing information. In such cases, accountability and privacy may appear to be in conflict. Accountability means identifying the source of a transaction, while privacy might deny meaningful identification. These objectives can be reconciled with care. Accountability protects everyone—for example, where a seller has a legitimate need to authenticate the identity of a buyer for credit purposes, while the holder of the credit card has a legitimate need to authenticate the seller to prevent fraudulent misrepresentation.

To support accountability, information must be sufficient, accurate, timely, and available to management to meet its responsibilities. To help ensure reliability of information, the auditor evaluates controls over unacceptable processing and reporting. Some of these controls are listed next.

- Information can be supported irrefutably. Controls that provide support are variously known as transaction trails or audit trails.
- Information should be timely. It must be available when decisions are made. This is a common criticism of financial statements issued months after the events.
- Information must be consistent, in accordance with applicable policies. Errors of inappropriate processing, whether programmed or not, are common causes of this effect. Management override can be another.

(ii) ITGI's COBIT

The control objectives make a clear and distinct link to business objectives in order to support significant use outside the audit community. Control objectives are defined in a process-oriented manner following the principle of business reengineering.

An internal control system or framework must be in place to support business processes, and it must be clear how each individual control activity satisfies the information requirements and impacts the resources. Impact on IT resources is highlighted in the COBIT framework together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information that need to be satisfied. Control, which includes policies, organizational structures, practices, and procedures, is management's responsibility. Management, through its corporate governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance, or operation of information systems.

Business orientation is the main theme of COBIT. It is designed not only to be employed by users and auditors but also—and more important—as a comprehensive checklist for business process owners. Increasingly, business practice involves the full empowerment of business process owners

as they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. The COBIT framework provides a tool for the business process owner that facilitates the discharge of this responsibility.

The COBIT framework starts from a simple and pragmatic premise: In order to provide the information that the organization needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The COBIT framework includes (1) the classification of domains where high-level control objectives apply (domains and processes), (2) an indication of the business requirements for information in that domain, and (3) the IT resources primarily impacted by the control objectives.

COBIT continues with a set of high-level control objectives, one for each of the IT processes, grouped into four domains:

1. Planning and organization
2. Acquisition and implementation
3. Delivery and support
4. Monitoring

In establishing the list of business requirements, COBIT combines the principles embedded in existing and known reference models.

- Quality requirements cover quality, cost, and delivery.
- Fiduciary requirements (COSO report) cover effectiveness and efficiency of operations, reliability of information, and compliance with laws and regulations.
- Security requirements cover confidentiality, integrity, and availability.

The COBIT framework consists of high-level control objectives and an overall structure for their classification. The underlying theory behind the classification is three levels of IT efforts when considering the management of IT resources (see Exhibit 6.8). Starting at the bottom, there are activities and tasks needed to achieve a measurable result. Activities have a life cycle concept while tasks are more discrete. The life cycle concept has typical control requirements that are different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains.

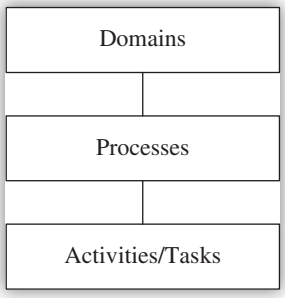


EXHIBIT 6.8 COBIT Classification System

- **Domain 1: Planning and organization.** This domain covers strategy and tactics and concerns the identification of the ways IT can best contribute to the achievement of business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated, and managed for different perspectives. Finally, a proper organization as well as a technological infrastructure must be put in place.
- **Domain 2: Acquisition and implementation.** To realize the IT strategy, IT solutions need to be identified, developed, or acquired as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.
- **Domain 3: Delivery and support.** This domain is concerned with the actual delivery of required services, which range from traditional operations of security to the continuity of training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
- **Domain 4: Monitoring.** All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

In summary, in order to provide the information that the organization needs to achieve its objectives, the organization must exercise IT governance to ensure that IT resources are managed by a set of naturally grouped IT processes.

(iii) ISACF's CONCT

CONCT, issued by the ISACF, focuses on these activities: intranet, extranet, Internet; data warehouses; and online transaction processing systems (TPSs). CONCT provides well-structured ways of understanding and assessing the very complex centric technology environment that exists.

The IT governance model for centric technology has three dimensions: IT control objectives for information services, IT activities, and the IT resources required for the accomplishment of these activities.

(iv) AICPA/CICA SysTrust Principles and Criteria for Systems Reliability

Several organizations, such as AICPA/CICA, provide guidance on information security in terms of principles, standards, management, assurance, and measurement.

SysTrust is an assurance service designed to increase the comfort of management, customers, and business partners with the systems that support a business or a particular activity. The SysTrust service entails a public accountant providing an assurance service in which he or she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity, and maintainability. For each of the four principles, 58 reliability criteria have been established against which a system can be evaluated.

Potential users of this service are shareholders, creditors, bankers, business partners, third-party users who outsource functions to other entities, stakeholders, and anyone who in some way relies on the continued availability, integrity, security, and maintainability of a system. The SysTrust service will help differentiate entities from their competitors because entities that undergo the rigors of a SysTrust engagement will presumably be better service providers—attuned to the risks posed by their environment and equipped with the controls that address those risks.

(v) IFAC's Managing Security of Information

International Information Technology Guidelines are issued by the IFAC, Information Technology Committee.

Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. Threats may emanate from, among others, technical conditions (e.g., program bugs and disk crashes), natural disasters (e.g., fires and floods), environmental conditions (e.g., electrical surges), human factors (e.g., lack of training, errors, and omissions), unauthorized access (e.g., hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third-party communications carriers, outsourced operations), that can potentially result in a loss of management control and oversight are increasing in significance.

The objective of information security is the protection of the interest of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity. For any organization, the security objective is met when:

- Information systems are available and usable when required (availability objective).
- Data and information are disclosed only to those who have a right to know it (confidentiality objective).
- Data and information are protected against unauthorized modification (integrity objective).

The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information systems and the business context in which it is used. Core information security principles presented by the IFAC are derived from the Guidelines published by the OECD.

(vi) ISF Standard

The ISF's standard of good practices for information security is based on research and the practical experience for forum members. The standard divides security into five component areas:

1. Security management
2. Critical business applications
3. Computer installations
4. Networks
5. System development

(vii) U.S. Department of Homeland Security

The U.S. Department of Homeland Security cohosted a National Cyber Security Summit in 2003 and formed five task forces, including the Corporate Governance Task Force. In its report, the task force called on all organizations to make information security governance a corporate board-level priority. The report requires COSO of the Treadway Commission to revise its document entitled "Internal Controls—An Integrated Framework" so it explicitly addresses information security governance.

(viii) EU's Security Directives
The EU has issued several directives covering:

- Information security
- Attacks against information systems
- Legal aspects of electronic commerce
- Access to electronic communications networks
- Protection of personal data
- Safer Internet Plus Programme (i.e., no illegal or harmful content)
- Unfair commercial practices
- Copyrights in the information society
- International safe harbor privacy principles

(ix) OECD's Guidelines for the Security of Information Systems
The OECD has developed critical information infrastructure framework and has issued several guidelines as they relate to information technology and information security. These guidelines cover data collection limitations, quality of data, limitations on data use, IT security safeguards, accountability of the data controller, trans-border data flow laws dealing with personal data, cross-border threats, privacy laws, cryptography guidelines, anti-spam regulations, electronic authentication guidelines and cross-border cooperation in the enforcement of laws protecting privacy.

(x) International Common Criteria
The CC is a product evaluation model that represents the outcome of efforts to develop criteria for evaluation of IT security. These criteria will be used throughout the international community. The CC defines a set of IT requirements of known validity used in establishing security requirements for prospective products and systems. The CC also defines the "protection profile" construct that allows prospective consumers or developers to create standardized sets of security requirements that will meet their needs. The CC presents requirements for the IT security of a product under the distinct categories of functional requirements and assurance requirements (www.commoncriteriaportal.org).

Examples of functional requirements include requirements for identification and authentication and security classes of products and systems. In essence, the CC is a standard security specification "language." Products whose security properties have been specified using the CC may then be validated (tested) for conformance to their CC specifications. Such a validation, when performed by an accredited testing laboratory, confirms that the product meets its security specification(s). Note that ISO/IEC (International Electrotechnical Commission) standard 15408 addresses the CC in the form of evaluation criteria for IT security.

The CC is a repeatable methodology for documenting IT security requirements, documenting and validating product security capabilities, and promoting international cooperation in the IT security area. It supports security in depth and security layering concepts.

Using CC protection profiles and security targets greatly aids the development of products or systems that have IT security functions. The rigor and repeatability of the CC methodology provides thorough definition of user security needs. Validated security targets provide system

integrators with key information needed to procure security components and implement secure IT functions and features.

The protection profile (PP) contains a set of security requirements either from the CC or stated explicitly, which should include evaluation assurance levels (EALs). The security target (ST) contains a set of security requirements that may be made by reference to a protection profile, directly by reference to CC functional or assurance components, or stated explicitly.

The CC permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. The evaluation results may help consumers to determine whether these IT products fulfill their security needs. The CC is useful as a guide for the development, evaluation, and/or procurement of products with IT security functionality.

The CC uses the term "product" to refer to an IT product, a part of an IT product, and a set of IT products. Examples of IT products are listed next.

- A software application
- An operating system (OS)
- A software application in combination with an OS
- A software application in combination with an OS and a workstation
- An OS in combination with a workstation
- A smart card integrated circuit
- The cryptographic coprocessor of a smart card integrated circuit
- A local area network (LAN) including all terminals, servers, network equipment, and software
- A database application excluding the remote client software normally associated with that database application

The CC addresses protection of information from unauthorized disclosure (confidentiality), modification (integrity), or loss of use (availability). The CC is also applicable to risks arising from human activities (malicious or otherwise) and to risks arising from nonhuman activities. The CC is applicable to IT security functionality implemented in hardware, firmware, or software.

Because the next topics involve specialized techniques or because they are somewhat peripheral to IT security, they are considered to be outside the scope of the CC:

- The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. Administrative security controls, such as organizational, personnel, physical, and procedural controls, are important in other areas.
- The evaluation of technical physical aspects of IT security, such as electromagnetic emanation control, is not specifically covered. The CC does address some aspects of physical protection.

- The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be applied by evaluation authorities.
- The procedures for use of evaluation in accreditation are outside the scope of the CC. The results of the evaluation process are an input to the accreditation process.
- The CC does not cover the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms.
- The CC does not state requirements for the regulatory framework.

By establishing a CC base, the results of an IT security evaluation will be meaningful to a wider audience. There are three groups with a general interest in evaluation of the security properties of target of evaluations (TOEs): consumers, developers, and evaluators. The CC gives consumers, especially in consumer groups and communities of interest, an implementation-independent structure termed the "protection profile" (PP) in which to express their special security requirements. The CC is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the security target (ST). This ST may be based on one or more PPs. The CC contains criteria to be used by evaluators when forming judgments about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out but does not specify procedures to be followed in carrying out those actions.

Some of the additional interest groups that can benefit from information contained in the CC are listed next.

- System custodians and system security officers responsible for determining and meeting organizational IT security policies and requirements
  - Auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution
  - Security architects and designers responsible for the specification of security properties of IT products
  - Accreditors responsible for accepting an IT solution for use within a particular environment
  - Sponsors of evaluation responsible for requesting and supporting an evaluation
- Evaluation authorities responsible for the management and oversight of IT security evaluation programs

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations, and administers the regulations to which the evaluation facilities and evaluators must conform.

Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgment and background knowledge for which consistency is more difficult to achieve. As the application of criteria contains objective and subjective elements, precise and universal ratings for IT security are infeasible.

The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval. It is noted that the certification process is a means of gaining greater consistency in the application of IT security criteria.

The evaluation scheme, methodology, and certification process are the responsibility of the evaluation authorities who run evaluation schemes and are outside the scope of the CC. However, the evaluation base is part of the CC.

The outcome of an evaluation is a statement about the extent to which assurance is gained that the TOE can be trusted to reduce the risks to the protected assets and does not itself possess exploitable vulnerabilities. The statement assigns an assurance rating to the TOE, assurance being that property of a TOE that gives grounds for confidence in its proper operation. This statement can be used by the asset owner in deciding whether to accept the risk of exposing the assets to the threats. This mandates that evaluation leads to objective and repeatable results that are defensible and can be cited as evidence.

(xi) ISO Standards

The ISO issues several standards to business, government, and society for economic, environmental, and social development. It develops standards for which there is a clear market requirement, as these standards provide specific solutions to achieve specific benefits. The ISO issued several standards relating to IT and information security, as follows.

ISO 27001:2005—*INFORMATION TECHNOLOGY SECURITY TECHNIQUES—REQUIREMENTS OF INFORMATION SECURITY MANAGEMENT SYSTEMS*

The ISO/IEC 27001:2005 standard covers all types of organizations (e.g., commercial enterprises, government agencies, and not-for-profit organizations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system within the context of organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. This standard use the Plan-Do-Check-Act (PDCA) cycle framework.

The ISO/IEC 27001:2005 standard is intended to be suitable for several different types of use, including use:

- Within organizations to formulate security requirements and objectives.
- Within organizations as a way to ensure that security risks are cost-effectively managed.
- Within organizations to ensure compliance with laws and regulations.
- Within organizations as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met.
- In definition of new information security management processes.
- In identification and clarification of existing information security management processes.
- By the management of organizations to determine the status of information security management activities.
- By the internal and external auditors of organizations to determine the degree of compliance with the policies, directives, and standards adopted by an organization.

- By organizations to provide relevant information about information security policies, directives, standards, and procedures to trading partners and other organizations with which they interact for operational or commercial reasons.
- In implementation of business-enabling information security.
- By organizations to provide relevant information about information security to customers.

ISO 27002:2005—*INFORMATION TECHNOLOGY SECURITY TECHNIQUES—CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT*

The ISO/IEC 27002:2005 standard (formerly known as ISO/IEC 17799 standard and the British Standard Institute's BS 7799 standard) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. This standard provides a comprehensive set of controls addressing information security, including security governance. It is intended to serve as a single reference point for identifying controls needed for most situations where information systems are used in industry and commerce for large, medium, and small organizations. The standard has three major components: confidentiality, integrity, and availability. The control objectives provide general guidance on the commonly accepted goals of information security management.

This standard contains best practices of control objectives and controls in the next areas of information security management:

- Security policy deals with management direction, including risk assessment.
- Organization of information security deals with governance of information security.
- Asset management deals with inventory and classification of information assets.
- HR security deals with security aspects for employees joining, in moving within, and leaving an organization.
- Physical and environmental security deals with protection of the computer facilities.
- Communications and operations management deals with management of technical security controls in systems and networks.
- Access control deals with restriction of access rights to networks, systems, applications, functions, and data.
- Information systems acquisition, development, and maintenance deals with building security into applications.
- Information security incident management deals with anticipating and responding appropriately to information security breaches.
- Business continuity management deals with protecting, maintaining, and recovering business-critical processes and systems.
- Compliance deals with ensuring conformance with information security policies, standards, laws, and regulations.

The control objectives and controls just listed are intended to be implemented to meet the requirements identified by a risk assessment. They are intended as a common basis and practical guidelines for developing organizational security standards and effective security management practices and to help build confidence in interorganizational activities.

ISO 28000 — *SECURITY MANAGEMENT SYSTEMS FOR THE SUPPLY CHAIN*

The ISO 28000:2007 standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Managers responsible for selecting suppliers for purchasing decisions can refer to ISO 9001 for the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain. Some examples of risks in the supply chain include piracy, fraud, and terrorism.

The ISO 28000:2007 standard is applicable to all sizes of organizations, from small to multinational, in manufacturing (including software and hardware), service, storage, or transportation at any stage of the production or supply chain that wishes to:

- Establish, implement, maintain, and improve a security management system.
- Assure conformance with stated security management policy.
- Demonstrate such conformance to others.
- Seek certification/registration of its security management system by an accredited third-party certification body.
- Alternately, make a self-determination and self-declaration of conformance with ISO 28000:2007. It is not the intention of ISO 28000:2007 to require duplicative demonstration of conformance. Organizations that choose third-party certification can further demonstrate that they are contributing significantly to supply chain security.

Other ISO Standards

- The ISO/IEC 15026 standard addresses software assurance in terms of managing risks and assuring safety, security, and dependability within the context of system and software life cycles.
- The ISO/IEC 15026-3:2011 standard addresses software assurance in terms of managing risks and assuring safety, security, and dependability within the context of system and software life cycles. This standard is intended for use by:
  - Definers of integrity levels, such as industry and professional organizations, standards organizations, and government agencies.
  - Users of integrity levels, such as developers and maintainers, suppliers and acquirers, users, assessors of systems or software, and for the administrative and technical support of systems and/or software products.
- The ISO/IEC 17025 standard addresses independent testing of software using either the white box or the black box testing method.
- The ISO/IES 22301 standard provides guidance on business continuity management, including IT contingency planning.
- The ISO/IEC 15048 standard addresses evaluation criteria for IT security (i.e., CC).
- The ISO/IEC 27003:2010 standard deals with IT security techniques regarding system implementation guidance in accordance with the ISO/IEC 27001:2005 standard.
- The ISO/IEC 27004:2009 standard deals with IT security techniques regarding measurement of controls in accordance with the ISO/IEC 27001:2005 standard.
- The ISO/IEC 27005:2011standard deals with IT security techniques regarding risk management in accordance with the ISO/IEC 27001:2005 standard.

- The ISO/IEC 27006 standard provides requirements for bodies providing audit and certification of information security management systems.
- The ISO/IEC 27007:2011 standard deals with IT security techniques regarding management systems auditing in accordance with the ISO 19011 standard and the ISO 19001 standard dealing with auditing management systems.
- The ISO/IEC 90003:2004 standard deals with software engineering guidelines for the application of ISO 9001:2000 to computer software. This standard provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation, and maintenance of computer software and related support services. This standard does not add to or otherwise change the requirements of ISO 9001:2000. These guidelines are not intended to be used as assessment criteria in quality management system (QMS) registration or certification. The application of ISO/IEC 90003:2004 is appropriate to software that is:
  - Part of a commercial contract with another organization.
  - A product available for a specific market sector.
  - Used to support the processes of an organization.
  - Embedded in a hardware product.
  - Related to software services.
- The ISO/IEC 18033 standard deals with encryption algorithms.
- The ISO/IEC 10116 standard deals with security techniques for modes of operation for an *n*-bit block cipher.
- The ISO/IEC 11770 standard deals with security techniques for cryptographic key management framework and mechanisms for using symmetric key techniques.

SUMMARY OF INFORMATION TECHNOLOGY CONTROL FRAMEWORKS

A summary of IT control frameworks presented in this section and more follows.

- **The IIA's eSAC** sets the stage for effective technology and risk management by providing a framework for evaluating the e-business control environment.
- **ITGI's COBIT** states that control objectives make a clear and distinct link to business objectives in order to support significant use outside the audit community. Control objectives are defined in a process-oriented manner following the principle of business reengineering. COBIT focuses on processes and process ownership; looks at fiduciary, quality, and security needs of enterprises; and provides seven information criteria in terms of what a business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability, and compliance.
- **ISACF's CONCT** focuses on intranet, extranet, and Internet; data warehouses; and online TPSs.
- **AICPA/CICA's SysTrust Principles and Criteria for Systems Reliability** provide guidance on information security in terms of principles, standards, management, assurance, and measurement.
- **IFAC's Managing Security of Information** states that the objective of information security is to protect the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity.

- **The ISF Standard** divides security into five component areas:
  1. Security management
  2. Critical business applications
  3. Computer installations
  4. Networks
  5. System development
- **The U.S. Department of Homeland Security's** task force on corporate governance calls on all organizations to make information security governance a corporate board-level priority.
- **The EU's Security Directives** cover these areas:
  - Information security
  - Attacks against information systems
  - Legal aspects of electronic commerce
  - Access to electronic communications networks
  - Protection of personal data
  - Safer Internet Plus Programme (i.e., no illegal or harmful content)
  - Unfair commercial practices
  - Copyrights in the information society
  - International safe harbor privacy principles
- **OECD's Guidelines for the Security of Information Systems** cover these areas:
  - Data collection limitations
  - Quality of data
  - Limitations on data use
  - IT security safeguards
  - Accountability of the data controller
  - Transborder data flow laws dealing with personal data
  - Cross-border threats
  - Privacy laws
  - Cryptography guidelines
  - Antispam regulations
  - Electronic authentication guidelines
  - Cross-border cooperation in the enforcement of laws protecting privacy
- **International CC** is a product evaluation model that represents the outcome of efforts to develop criteria for evaluation of IT security. These criteria is used throughout the international community.
- **The ISO** issues several standards to business, government, and society for economic, environmental, and social development throughout the world. The two popular ISO standards related to IT include ISO 27001—*Information Security Management Techniques—Requirements* and

ISO 27002— *Information Security Management Techniques—Code of Practice for Information Security Management*, which consists of three major components: confidentiality, integrity, and availability.

- The minimum security requirements are expressed in terms of management, operational, and technical controls.
- The CICA's ITCG provides security guidelines.
- The U.K. Office of Government Commerce (OGC), Information Technology Infrastructure Library (ITIL), Security Management, provides security guidelines.

(ix) Minimum Security Requirements

Regardless of the control framework used, there are 17 minimum security requirements that all IT organizations should adhere to. These security requirements are expressed in terms of security safeguards or controls. Security controls are the management, operational, and technical safeguards and countermeasures that are needed to protect the confidentiality, integrity, and availability of a computer system and its information. *Management safeguards* or controls range from risk assessments to security planning. *Operational safeguards* or controls include factors such as personnel security and basic hardware/software maintenance. *Technical safeguards* or controls include items such as audit trails and communications protection. These security controls constitute the minimum security requirements for information systems and the information processed, stored, and transmitted by those systems.[3]

Management Controls

1. **Risk assessment.** Organizations must periodically assess the risk to organizational operations (including mission, function, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
2. **Planning.** Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and rules of behavior for individuals accessing the information systems.
3. **Systems and services acquisition.** Organizations must:
   - **a.** Allocate sufficient resources to adequately protect organizational information systems.
   - **b.** Employ SDLC processes that incorporate information security considerations.
   - **c.** Employ software usage and installation restrictions.
   - **d.** Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
4. **Certification, Accreditation, and Security Assessments**: Organizations must:
   - **a.** Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

[3] *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200, U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, March 2006.

b. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

c. Authorize the operation of organizational information systems and any associated information system connections.

d. Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Operational Controls

5. **Personnel security.** Organizations must:
   a. Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.
   b. Ensure that organizational information and information systems are protected during and after personnel actions, such as terminations and transfers.
   c. Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
6. **Physical and environmental protection.** Organizations must:
   a. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.
   b. Protect the physical plant and support infrastructure for information systems.
   c. Provide supporting utilities (e.g., heating, air conditioning, and humidity levels) for information systems.
   d. Protect information systems against environmental hazards.
   e. Provide appropriate environmental controls in facilities containing information systems.
7. **Contingency planning.** Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
8. **Configuration management.** Organizations must:
   a. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective SDLCs.
   b. Establish and enforce security configuration settings for IT products employed in organizational information systems.
9. **Maintenance.** Organizations must:
   a. Perform periodic and timely maintenance on organizational information systems.
   b. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

10. **System and information integrity.** Organizations must:
    a. Identify, report, and correct information and information system flaws in a timely manner.
    b. Provide protection from malicious code at appropriate locations within organizational information systems.
    c. Monitor information system security alerts and advisories and take appropriate actions in response.
11. **Media protection.** Organizations must:
    a. Protect information system media, both paper and digital.
    b. Limit access to information on information system media to authorized users.
    c. Sanitize or destroy information system media before disposal or release for reuse.
12. **Incident response.** Organizations must:
    a. Establish an operational incident handling capability for organizational information systems that include adequate preparation, detection, analysis, containment, recovery, and user response activities.
    b. Track, document, and report incidents to appropriate organizational officials and/or authorities.
13. **Awareness and training.** Organizations must:
    a. Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to security of organizational information systems.
    b. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Technical Controls

14. **Identification and authentication.** Organizations must identify information system users, processes, acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.
15. **Access control.** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
16. **Audit and accountability.** Organizations must:
    a. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized or inappropriate information system activity.
    b. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

17. **System and communications protection.** Organizations must:
    a. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
    b. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

SUMMARY OF MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS DEFINED AS MINIMUM SECURITY REQUIREMENTS

Management controls include risk assessment; planning; systems and services acquisition; and certification, accreditation, and security assessments.

Operational controls include personnel security; physical and environmental protection; contingency planning; configuration management; maintenance; system and information integrity; media protection; incident response; and awareness and training.

Technical controls include identification and authentication; access control; audit and accountability; and system and communications protection.

(b) Operating Systems, Mainframe Computers, Terminals, Workstations, and Servers

In this section, highly interrelated and integrated topics—OSs, mainframe computers, terminals, workstations, and servers—are discussed because they all work together to process users' data with their vast amount of computing power. In addition, security over Web servers is highlighted in terms of their security levels and security controls.

(i) Operating Systems

An OS is an integrated collection of software routines that service the sequencing and processing of computer programs by a computer and is often called systems software. Many control operations are concentrated in systems software, which is defined as a collection of programs or systems that help interconnect and/or control the elements of input devices, computer processing operations, output devices, data files, application programs, and hardware. Typically, systems software is provided by outside vendors.

The OS may provide many services, such as computer resource allocation, computer job scheduling, input/output (I/O) control, and data management. The OS software controls the allocation and usage of hardware resources such as memory, central processing unit (CPU) time, disk space, and peripheral devices. The OS is often called the brain of a computer, whether it is a mainframe computer, personal computer (PC), desktop computer, palm computer, laptop computer, tablet computer, or mobile devices (e.g., smartphones, digital pads and tablets, and personal digital assistants [PDAs]). The OS is the foundation software on which applications software depends. Popular OSs for workstations include Windows, Mac OS, Linux, and UNIX. Network connectivity devices such as routers have their proprietary OSs, PDAs often run on specialized OSs, and many embedded systems, such as cell phones, digital cameras, and audio players, also use OSs. Although OSs are predominantly software based, partial or full implementations can be made in hardware in the form of **firmware**.

An OS is a program that runs on a computer and provides a software platform on which other programs can run. In addition, an OS is responsible for processing input commands from a user, sending output to a display, interacting with storage devices to store and retrieve data, and controlling peripheral devices, such as printers and modems.

OS data exist in both nonvolatile and volatile states. "Nonvolatile data" is data that persists even after a computer is powered down, such as a file system stored on a hard drive. "Volatile data" is data on a live system that is lost after a computer is powered down, such as the current network connections to and from the system. *Both types of data are useful to internal auditors when they perform IT system audits.*

(A) Nonvolatile Data The primary source of non-volatile data within an OS is the file system. The file system is also usually the largest and richest source of data within the OS, containing most of the information recovered during a typical forensic event. The file system provides storage for the OS on one or more media. It typically contains many types of files, each of which may be of value to analysts in different situations. In addition, important residual data can be recovered from unused file system space. Several types of nonvolatile data commonly found within OS file systems are listed next.

- **Configuration files**. The OS may use configuration files to store OS and application settings. For example, configuration files could list the services to be started automatically after system boot and specify the location of log files and temporary files. Users might also have individual OS and application configuration files that contain user-specific information and preferences, such as hardware-related settings (e.g., screen resolution and printer settings) and file associations. Configuration files can contain users and groups, password files, and scheduled jobs.
- **Users and groups.** The OS keeps a record of its user accounts and groups. Account information may include:
  - Group membership.
  - Account name and description.
  - Account permissions.
  - Account status (e.g., active, disabled).
  - Path to the account's home directory.
- **Password files.** The OS may store password hashes in data files. Various password-cracking utilities may be used to convert a password hash to its cleartext equivalent for certain OSs.
- **Scheduled jobs.** The OS maintains a list of scheduled tasks that are to be performed automatically at a certain time (e.g., perform a virus scan every week). Information that can be gleaned from this list include the task name, the program used to perform the task, command line switches and arguments, and the days and times when the task is to be performed.
- **Logs.** OS log files contain information about various OS events and may also hold application-specific event information. Depending on the OS, logs may be stored in text files, proprietary-format binary files, or databases. Some OSs write log entries to two or more separate files. The OS logs can contain this information:
  - Systems events
  - Audit records

- Application events
- Command history
- Recently accessed files
- Application files
- Data files
- Swap files
- Dump files
- Hibernation files
- Temporary files

- **System events.** System events are operational actions performed by OS components, such as shutting down the system or starting a service. Typically, failed events and the most significant successful events are logged, but many OSs permit system administrators to specify which types of events will be logged. The details logged for each event also vary widely. Each event is usually time-stamped; other supporting information could include event codes, status codes, and usernames.
- **Audit records.** Audit records contain security event information, such as successful and failed authentication attempts and security policy changes. OSs typically permit system administrators to specify which types of events should be audited. Administrators also can configure some OSs to log successful, failed, or all attempts to perform certain actions.
- **Application events.** Application events are significant operational actions performed by applications, such as application startup and shutdown, application failures, and major application configuration changes.
- **Command history.** Some OSs have separate log files (typically for each user) that contain a history of the OS commands performed by each user.
- **Recently accessed files.** An OS might log the most recent file accesses or other usage, creating a list of the most recently accessed files.
- **Application files**. Applications can be composed of many types of files, including these:
  - Executables
  - Scripts
  - Documentation
  - Configuration files
  - Log files
  - History files
  - Graphics
  - Sounds
  - Icons

- **Data files**. Data files store information for applications. Examples of common data files are listed next.
  - Text files
  - Word processing documents
  - Spreadsheets
  - Databases
  - Audio files
  - Graphics files

  In addition, when data are printed, most OSs create one or more temporary print files that contain the print-ready version of the data.
- **Swap files**. Most OSs use swap files in conjunction with random access memory (RAM) to provide temporary storage for data often used by applications. Swap files essentially extend the amount of memory available to a program by allowing pages (or segments) of data to be swapped in and out of RAM. Swap files may contain a broad range of OS and application information, such as usernames, password hashes, and contact information.
- **Dump files**. Some OSs have the ability to store the contents of memory automatically during an error condition to assist in subsequent troubleshooting. The file that holds the stored memory contents is known as a dump file.
- **Hibernation files**. A hibernation file is created to preserve the current state of a system (typically a laptop) by recording memory and open files before shutting off the system. When the system is next turned on, the state of the system is restored.
- **Temporary files**. During the installation of an OS, application, or OS or application updates and upgrades, temporary files are often created. Although such files typically are deleted at the end of the installation process, this does not always occur. In addition, temporary files are created when many applications are run; again, such files are usually deleted when the application is terminated, but this does not always happen. Temporary files could contain copies of other files on the system, application data, or other information.

Although file systems are the primary source of nonvolatile data, another source of interest is the Basic Input/Output System (BIOS). The BIOS contains many types of hardware-related information, such as the attached devices (e.g., CD-ROM drives and hard drives), the types of connections and interrupt request line assignments (e.g., serial, Universal Serial Bus [USB], and network card), motherboard components (e.g., processor type and speed, cache size, and memory information), system security settings, and hot keys. The BIOS also communicates with redundant array of independent disk (RAID) drivers and displays the information provided by the drivers. For example, the BIOS views a hardware RAID as a single drive and a software RAID as multiple drives. The BIOS typically permits the user to set passwords, which restrict access to the BIOS settings and may prevent the system from booting if the password is not supplied. The BIOS also holds the system date and time.

(B) Volatile Data OSs execute within the RAM of a system. While the OS is functioning, the contents of RAM are constantly changing. At any given time, RAM might contain many types of data and information that could be of interest. For example, RAM often contains frequently and recently accessed data, such as data files, password hashes, and recent commands. In addition,

like file systems, RAM can contain residual data in slack and free space. Other significant types of volatile data that might exist within an OS include network configuration, network connections, running processes, open files, login sessions, and OS time.

Slack Space Memory slack space is much less deterministic than file slack space. For example, an OS generally manages memory in units known as pages or blocks and allocates them to requesting applications. Sometimes, although an application might not request an entire unit, it is given one anyway. Residual data could therefore reside in the unit of memory allocated to an application, although it might not be addressable by the application. For performance and efficiency, some OSs vary the size of the units they allocate, which tends to result in smaller memory slack spaces.

Free Space Memory pages are allocated and deallocated much like file clusters. When they are not allocated, memory pages are often collected into a common pool of available pages, a process often referred to as garbage collection. It is not uncommon for residual data to reside in these reusable memory pages, which are analogous to unallocated file clusters.

Network Configuration Although many elements of networking, such as network interface card (NIC) drivers and configuration settings, are typically stored in the file system, networking is dynamic in nature. For example, many hosts are assigned Internet Protocol (IP) addresses dynamically by another host, meaning that their IP addresses are not part of the stored configuration. Many hosts also have multiple network interfaces defined, such as wired, wireless, virtual private network (VPN), and modem; the current network configuration indicates which interfaces are currently in use. Users also may be able to alter network interface configurations from the defaults, such as manually changing IP addresses. Accordingly, analysts should use the current network configuration, not the stored configuration, whenever possible.

Network Connections The OS facilitates connections between the system and other systems. Most OSs can provide a list of current incoming and outgoing network connections, and some OSs can list recent connections as well. For incoming connections, the OS typically indicates which resources are being used, such as file shares and printers. Most OSs can also provide a list of the ports and IP addresses at which the system is listening for connections.

Running Processes Processes are the programs that are currently executing on a computer. Processes include services offered by the OS and applications run by administrators and users. Most OSs offer ways to view a list of the currently running processes. This list can be studied to determine the services that are active on the system, such as a Web server, and the programs that individual users are running (e.g., encryption utility, word processor, and e-mail client). Process lists may also indicate which command options were used. Identifying the running processes is also helpful for identifying programs that should be running but have been disabled or removed, such as antivirus software and firewalls.

Open Files OSs may maintain a list of open files, which typically includes the user or process that opened each file.

Login Sessions OSs typically maintain information about currently logged in users (and the start time and duration of each session), previous successful and failed logons, privileged usage, and impersonation. However, login session information might be available only if the computer has been configured to audit logon attempts. Logon records can help to determine a user's computer usage habits and confirm whether a user account was active when a given event occurred.

Operating System Time The OS maintains the current time and stores daylight savings time and time zone information. This information can be useful when building a timeline of events or correlating events among different systems. Analysts should be aware that the time presented by the OS might differ from that presented by the BIOS because of OS-specific settings, such as time zone.

(C) OS Response to Failures OS response to failures can be classified into three general categories: system reboot, emergency system restart, and system cold start.

System reboot is performed after shutting down the system in a controlled manner in response to a trusted computing base (TCB) failure. For example, when the TCB detects the exhaustion of space in some of its critical tables or finds inconsistent object data structures, it closes all objects, aborts all active user processes, and restarts with no user process in execution. Before restart, however, the recovery mechanisms make a best effort to correct the source of inconsistency. Occasionally the mere termination of all processes frees up some important resources, allowing restart with enough resources available. Note that system rebooting is useful when the recovery mechanisms can determine that TCB and user data structures affecting system security and integrity are, in fact, in a consistent state.

Emergency system restart is done after a system fails in an uncontrolled manner in response to a TCB or media failure. In such cases, TCB and user objects on nonvolatile storage belonging to processes active at the time of TCB or media failure may be left in an inconsistent state. The system enters maintenance mode, recovery is performed automatically, and the system restarts with no user processes in progress after bringing up the system in a consistent state.

System cold start takes place when unexpected TCB or media failure takes place and the recovery procedures cannot bring the system to a consistent state. TCB and user objects may remain in an inconsistent state following attempts to recover automatically. Intervention of administrative personnel is now required to bring the system to a consistent state from maintenance mode.

(ii) Mainframe Computers, Terminals, and Workstations

OS software, mainframe computers, PCs, terminals, workstations, and servers are tightly connected in a network, and they work in a harmonious ways in handling computing jobs and services.

- **Mainframe computers.** Mainframe computers are big computers in terms of their memory, size, speed, and processing power. They are suitable to handling heavy-duty computing tasks required in databases and complex networks. They have the ability to support many users connected to the computer by terminals. Other computers, such as PCs and terminals, are connected to the mainframe computer to share resources and computing power.
- **Terminals**. A terminal is a networking device consisting of a video adapter, a monitor, and a keyboard. It is capable of sending and/or receiving information over a communications channel. A terminal does little no or no computer processing on its own; instead, it is connected to a computer with a communications link over a cable.
- **Workstations**. A workstation is a hardware device and is defined in several ways depending on its configuration. Several variations of configurations are discussed next. A workstation can be:
  - A combination of input, output, and computing hardware that an individual can use for work.

- A powerful stand-alone computer used in computer-aided design work requiring heavy-duty calculations and graphics.
- A PC or terminal connected to a network.

Workstations also can provide an operator–system interface, and they may not require external access.

(iii) Servers

A server is a host computer that provides one or more services for other hosts over a network as a primary function. A server is deployed in several ways, as discussed next. A server can be:

- A computer or device on a network that manages network resources such as files, programs, and data.
- A computer program that provides services to other computer programs in the same or another computer.
- A computer program running a server program and is based on client/server architecture, where the server software receives requests from the client, processes the requests, and returns data to the client.
- A computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network.

One of the most common motivations for using a server is resource sharing. The goal is to provide transparent access to organization-wide data distributed across PCs and mainframe computers while protecting the security and integrity of that data.

The database management system (DBMS) handles the logical organization of the data and communicates with the server OS to access the data storage devices. Servers can be either a LAN database server or a host database accessed via a gateway. The network OS provides software connectivity between the server database management systems software and the LAN.

There are many types of servers, and each server has its own specific purpose. Servers pose specific risks due to concentration of data in one place. For example, a file server is a computer and storage device for storing files; a Web server for access to Web content, a DNS server for domain name services, a database server for access to relational tables, and an e-mail server for access to e-mail services.

Today's servers are very powerful and fast and perform diverse functions, such as transferring files, storing data, communicating outside the network, and processing databases. Because a LAN server is charged with moving large quantities of data from disk and memory onto the network, it is by nature I/O bound rather than computer bound, resulting in degraded performance. One way to curb memory operations is with caching**,** a performance-enhancing technique that establishes a small, very-high-speed static RAM cache (or buffer) between main memory and the processor. This approach frees the LAN server from repeated calls to memory. The next time the processor goes looking for data, it first tries to retrieve it from cache memory.

Basically, servers are of two types: dedicated and nondedicated. The choice depends on the significance and risk level of the work done on the network.

In a **dedicated server**, the computer running the server software cannot be used as a workstation, hence the name "dedicated." **Advantages** of dedicated servers include: (1) They are easier to manage because all data are in one place, and (2) they are faster to run because servers do not have a local user to serve. **Disadvantages** of dedicated servers include that (1) it is harder to make resources available on an ad hoc basis because setting up a server is difficult and time consuming; and (2) if the server fails, all users are forced to discontinue their work because all resources are centralized (i.e., all users either work or do not work).

A **nondedicated server** can work as both a computer and a workstation. **Advantages** of nondedicated servers include: (1) They allow flexibility to users because users can make resources available on their computers as necessary; and (2) they make users LAN-literate, requiring them to take some administrative responsibilities for system backup and security. Item (2) can be viewed as either an advantage or a disadvantage, because users now can be network administrators. Convenience is the advantage, and unlimited access to system resources is the disadvantage of being a network administrator. **Disadvantages** of nondedicated servers include that (1) servers can suffer some performance degradation when being used simultaneously as workstations and computers; and (2) users must be LAN-literate, requiring them to back up the shared data, set up security, and establish access rights to the system.

HOW TO DECIDE BETWEEN A DEDICATED SERVER AND A NONDEDICATED SERVER

- Multitasking OSs require a dedicated file server.
- Single-task OSs require a nondedicated file server.

A number of specific servers are described next.

File servers send and receive data between a workstation and the server. A file server is the heart of a LAN. Its primary purpose is to make files, printers, and plotters available to users. The file server has to transfer the entire file across the network in order to process it. In a file server approach, each workstation has to provide the services of both a front end and a back end. The bandwidth is limited too. For these reasons, database servers are better. A file server cannot be a diskless workstation. An FTP server is an example of a file server. In mobile devices, the FTP server could result in arbitrary code execution, which is a risky situation. Possible mitigations include installing patches and software updates.

Database servers (e.g., SQL) can access data from mainframes, minicomputers, and other servers, providing a critical link in distributed database systems. They employ client/server architecture for application systems in a distributed computing environment. Distributed computing enables a standard set of resources and services (i.e., directories, files, print queues, named pipes, communications queues, data, and programs) residing on different machines in different locations to be available to any workstation connected to the network. Simply stated, the client part of the client/server issues a request to the server, and the server part processes the request and returns the requested information to the client.

Client/server architecture makes it possible for a wide range of front-end client applications, such as databases, spreadsheets, and word processors, to share the same data simultaneously.

A database server supports a high-performance, multi-user, relational database management system (RDBMS). Client/server architecture provides a high level of data integrity, concurrency control, and improved performance.

The database server's distributed update capability allows databases on multiple database servers located in different places to be updated by a single transaction. This ability to scale a system in response to database server requirements provides greater flexibility in accessing geographically dispersed data. Some database servers provide transaction buffering, automatic disk repair, and a real-time tape backup option to guard against hardware problems.

Print servers allow multiple users and multiple PCs to share an expensive printer, such as a high-speed and high-quality laser printer, and a plotter. The spooling software may come with the printer software to queue jobs ready to be printed.

Communication servers (terminal servers) allow LANs to be connected to WANs and enable a stand-alone PC to connect directly to a WAN. Communications servers share LAN user files and password files. The terminal server is a dedicated computer with an asynchronous communications controller and a network interface. Its job is to take keystrokes entered by a user and deliver them to one or more host computers on a network. Terminal servers tie together character-based terminals, printers, and their host computers. An example is a terminal server giving each teleworker access to a separate standardized virtual desktop. The terminal server simulates the look and feel of a desktop OS and provides access to applications.

A communications server can be used to provide interconnectivity between all managed network elements and the out-of-band management (OOBM) gateway router for administrative access to the device's console port. In the event the OOBM network is not able to provide connectivity due to an outage, the communications server can provide a dial-up, point-to-point protocol (PPP) connection to access a network element. The auxiliary port, console port, and low-speed asynchronous serial port with an analog modem connected to the managed device also provides the capability for direct dial-up administrative access for infrastructures that do not have a communications server for management access.

Facsimile (fax) servers allow a single user or many users to transmit high-quality and high-volume documents straight from the PC or workstation disk without passing the document through the scanner of a stand-alone fax machine. Documents can be sent to and received from any fax machine. With fax modules integrated into the system, both background (fax application) and foreground (other application) processing can take place simultaneously, which increases productivity.

Image servers store and process documents, such as loan, credit, and employment applications, invoices, and purchase orders. Stored documents can be retrieved later and/or further transmitted to the host computer, or downloaded to a PC.

Network servers (super servers) connect LAN users to host (e.g., mainframe) computer sessions and public data networks. These interconnections become fully transparent to users. Super servers are hardware-based, unlike others that are software-based (e.g., disk mirroring). Fault tolerance is a major feature of these servers, using techniques such as disk duplexing. Network servers can handle heavy traffic generated by hundreds or thousands of users with faster I/O rates, and they usually come with more disk space.

Mail servers are a part of a network, acting as the central electronic mail (e-mail) drop for a set of users (i.e., an electronic post office). All e-mail messages are routed to this server, which delivers them to the addressees. The recipients run their e-mail program to read the message. E-mail servers can store and forward messages across all computing resources of an organization. E-mail servers and clients can be configured to block specific e-mail attachments with certain file extensions. This can help to reduce the likelihood of computer infections.

An **application server** is a computer responsible for hosting applications to user workstations. Application servers include directory services providing organization-wide distributed directories and document management services implementing a lending library concept that lets users "check out" documents for review and revision. Most server-level applications have extensive auditing capabilities, which can be of value in tracking down suspected or actual intrusions.

Redundant servers record data on two servers simultaneously. When the primary server fails for any reason, the backup server takes over.

X Window servers create and manipulate windows in response to requests from clients and send events to notify clients of user input or changes in a window's state. The server provides a portable layer between all applications and the display hardware. The X Window server typically runs on a workstation or PC with a graphics display, although some vendors offer dedicated X terminals that implement all or part of the X Window server in hardware or firmware.

Video servers are specialized versions of network servers. They store digitized video images (movies) that require far greater storage and network capacity than text files, and they distribute those images across LANs/WANs to desktop PCs. Video servers require higher levels of bandwidth to carry the data loads that video imposes. Zipf's law can be helpful in estimating the storage capacity of a video server for a movie distributor in storing movies. The law states that the most popular movie is seven times as popular as the seventh most popular movie. It is assumed that most customers will order the most popular movie more often.

Web servers on the Internet are providing knowledge bases in various organizations. These servers, connected through hyperlinks, provide a global interconnected document of knowledge bases permitting corporations, individuals, universities, and research centers all over the world to share and use common information. In other words, they make information more accessible and products more user friendly and easier to configure remotely. However, they may also add cyberrisks and create new security vulnerabilities that need to be addressed. For example, software components such as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. In addition, FTP and e-mail servers are used to configure remotely and to generate e-mail notifications when certain adverse conditions occur. From a strong security viewpoint, Hypertext Transfer Protocol Secure (HTTPS) should be used instead of HTTP, SFTP, or SCP should be used instead of FTP or TFTP and inbound FTP and e-mail traffic should be blocked.

HTTP server is server software that uses HTTP to serve up Hypertext Markup Language (HTML) documents and any associated files and scripts when requested by a client, such as a Web browser. The connection between client and server is usually broken after the requested document or file has been served. HTTP servers are used on Web and Intranet sites. HTTP servers are also called Web servers.

WHAT ARE SERVER-BASED THREATS?

Server-based threats occur due to poorly implemented session tracking, which may provide an avenue of attack. Similarly, user-provided input might eventually be passed to an application interface that interprets the input as part of a command, such as a SQL command. Attackers may also inject custom code into the website for subsequent browsers to process via cross-site scripting (XSS). Subtle changes introduced into the Web server can radically change its behavior (e.g., turning a trusted entity into malicious one), the accuracy of the computation (e.g., changing computational algorithms to yield incorrect results), or the confidentiality of the information (e.g., disclosing collected information).

Authentication servers can be used to solve identification and authentication problems in distributed systems. Third-party authentication based on Kerberos and X.509 certificates is widely used to communicate between previously unknown entities and across heterogeneous OSs. An authentication sever is used to distribute shared session keys to parties, and its responsibility is to authenticate the identity of entities in the network. Both Kerberos and X.509 certificates rely on reusable passwords where they are subjected to offline password cracking attacks. Other examples of authentication servers include RADIUS, TACACS, and DIAMETER, which are often labeled as authentication, authorization, and accounting (AAA) servers. Regardless of the type of authentication server used, an organization must install an intrusion detection system (IDS) to monitor the system for password cracking attacks.

Using standardized authentication protocols, such as RADIUS, TACACS+, and Kerberos, an authentication server provides centralized and robust authentication services for the management of network components. An authentication server is very scalable as it supports many user accounts and authentication sessions with the network components. It allows for the construction of template profiles or groups that are given authorization for specific tasks and access to specific resources. Users are then given an account that has been configured in the authentication server and has been assigned to a group.

Remote access servers/network access servers (RASs/NASs) are devices that provide for the initial entry point into a network. The NAS provides all the services that are normally available to a locally connected user (e.g., file and printer sharing and database and Web server access). Permission to dial into the local network is controlled by the NAS and can be granted to single users, groups, or all users. The RAS allows access to a network via a dial-up phone connection.

RAS and NAS devices can interface with authentication servers, such as RADIUS and TACACS. Regarding configuration of RAS or NAS, it is a sound approach to place dial-in users under the same access policy as those connecting via a VPN. This can be accomplished by placing the RAS either in the DMZ or within a screened subnet where the VPN gateway resides. The screened subnet architecture provides a layered defense. It ensures that only authorized users are permitted access to the internal network while still providing protection for the RAS. Only services that are needed should be allowed through the firewall from the RAS. The network administrator will ensure that logs provide a call audit trail and, if callback procedures are used, upon establishment of the callback connection, the communications device requires the user to authenticate to the system.

RASs are devices such as VPN gateways and modem servers that facilitate connections between networks. This often involves systems connecting to internal systems through the RAS but can also include internal systems connecting to external or internal systems. RASs typically record

the origin of each connection and might also indicate which user account was authenticated for each session. If the RAS assigns an IP address to the remote user, this is also likely to be logged. Some RAS also provide packet filtering functions, which typically perform logging similar to that provided by firewalls and routers. RASs typically work at a network level, supporting the use of many different applications. Because the servers have no understanding of the applications' functions, they usually do not record any application-specific data.

In addition to RASs, organizations typically use multiple applications that are specifically designed to provide remote access to a particular host's OSs. Examples include Secure Shell (SSH), TELNET, terminal servers, and remote control software. Such applications typically can be configured to log basic information for each connection, including source IP address and user account. Organizations also typically use many applications that are accessed remotely, such as client/server applications. Some of these applications also log basic information for connections. Although most remote access–related logging occurs on the RAS or the application server, in some cases the client also logs information related to the connection.

A **quarantine server** is used for protection at the network gateway from malicious code attacks. A common technique used in protecting networks is to use a firewall. In this technique, if a user attempts to retrieve an infected program via FTP, HTTP, or Simple Mail Transfer Protocol (SMTP), it is stopped at the quarantine server before it reaches the individual workstations. The firewall will direct suspicious traffic to the antivirus scanner on the quarantine server. This technique scales well since LAN administrators can add multiple firewalls or gateway scanners to manage network traffic for improved performance. In addition, users cannot bypass this architecture, and LAN administrators do not need to configure clients at their workstations. Other useful scanning techniques for a network include continuous, automated malicious code scanning using numerous scripts. Simple commands can be executed, and numerous computers in a network can be scanned for possible infections. Other scripts can be used to search for possible security holes through which future malicious code could attack the network. Only after fixing these security holes can a network withstand many attacks from malicious code.

WHAT IS A SERVER FARM AND HOW IS IT CONTROLLED?

A **server farm** is a physical security control that uses a network configuration mechanism to monitor and minimize theft of or damage to servers because all servers are kept in a single, secure physical location with a key and lock. If not controlled well, server farms can become a single point of failure and can be a target of internally originated attacks. Only those individuals (e.g., server administrators) who require physical access to the server farm should be given a key to open and close the doors. Two-person control is better.

Examples of logical security controls over a server farm include host- and network-based IDS, private virtual LANs (VLANs), access controls with strong passwords, and good system administration practices (e.g., keeping systems up to date with the latest patches).

A **virtual server** is built on the top of off-the-shelf servers for designing certification authority (CA) services. The virtual server can become very robust evidence of attacks on or mistakes made by other servers. Virtual servers are much easier to migrate between physical hosts in an infrastructure, and this movement may have unintended security consequences. For example, moving a virtual server from a lower-risk (more trusted) to a higher-risk (less trusted) domain may expose the sensitive information the server contains or is allowed to process unless its configuration is hardened appropriately. Conversely, when a virtual server is moved from a higher-risk

(less trusted) domain to a lower-risk (more trusted) domain, its hardening configuration may interfere with normal operation unless it is matched to that appropriate for the lower-risk domain.

A **DNS server** is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative DNS servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility).

Transport layer security (TLS) proxy servers provide network, transport, or application-layer VPNs (depending on the configuration). Typically, remote users connect to the proxy server using TLS-protected HTTP and authenticate themselves; the user can then access designated applications indirectly through the proxy server, which establishes its own separate connections with the application servers. Non–Web-based applications can be accessed by deploying special programs to clients and then tunneling the application data over HTTPS or another protocol; another method is to use a terminal server and to give users a Web-based terminal server client. Unlike Internet Protocol security (IPsec), TLS proxy servers cannot protect IP header characteristics, such as IP addresses. TLS/SSL proxy server provides a more robust VPN solution for remote users than other means.

HOW TO MAINTAIN SERVER INTEGRITY?

To ensure and maintain the integrity of the network servers, it is important to constantly monitor them for signs of malicious activity and other vulnerabilities. Integrity controls include a server farm, a secure DMZ, a secure server network with firewalls, or using routers behind the firewall.

A **network time protocol (NTP) server** is maintained to synchronize clocks and logs in different time zones throughout the world. NTP helps organizations with systems in multiple time zones to convert all logged times to a single time zone. NTP provides an efficient and scalable method for network elements to synchronize to an accurate time source referred to as the reference clock or stratum-0 server. The reference clock synchronizes to the Coordinated Universal Time (UTC) derived from a set of atomic clocks using Global Positioning System (GPS), code division multiple access (CDMA), or other time signals.

A **system log server** (a syslog server) provides the network administrator the ability to configure all of the communication devices on a network to send log messages to a centralized host for review, correlation, reporting, and storage. This implementation provides for easier management of network events and is an effective way to monitor and automatically generate alert notifications. The repository of messages facilitates troubleshooting when problems are encountered and can assist in performing root cause analysis. Syslog files can also be parsed in real time to identify suspicious behavior or be archived for review at a later time for research and analysis. Syslog is a protocol that specifies a general log entry format and a log entry transport mechanism.

A **management server** is a centralized device that receives information from the sensors or agents and manages them. The management server performs correlation analysis such as finding events triggered by the same IP address and identifies events that the individual sensors or agents cannot. Some small intrusion detection and prevention system (IDPS) deployments do not use any management servers, but most large IDPS deployments do. In large IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

A **Dynamic Host Configuration Protocol (DHCP) server** can be configured to log each IP address assignment and the associated media access control (MAC) address, along with a time-stamp. This information can be helpful to security analysts in identifying which host performed an activity using a particular IP address. However, analysts should be mindful of the possibility that attackers on an organization's internal networks falsified MAC or IP addresses, a practice known as spoofing.

DHCP is a set of rules used by communications devices, such as computers, routers, or network adapters, to allow the device to request and obtain an IP address from a server that has a list of addresses available for assignment. The DHCP service assigns IP addresses to hosts on a network as needed. Some hosts might have static IP addresses, meaning that they always receive the same IP address assignment; however, typically most hosts receive dynamic assignments. This means that the hosts are required to renew their IP address assignments regularly and that there is no guarantee that they will be assigned the same addresses. DHCP servers may contain assignment logs that include the MAC address, the IP address assigned to that MAC address, and the time the assignment occurred.

The MAC address, also known as the hardware address or Ethernet address, is a unique identifier specific to the network card inside a computer. MAC allows the DHCP server to confirm that the computer is allowed to access the network.

An **anonymizer server** is an intermediate server that performs activity on a user's behalf to preserve the user's privacy. Because IP addresses are often assigned dynamically, the system currently at a particular IP address might not be the same system that was there when the attack occurred. In addition, many IP addresses do not belong to end user systems but instead to network infrastructure components that substitute their IP address for the actual source address, such as a firewall performing network address translation. Some attackers use anonymizer servers.

A **Warez server** is a file server that is used to distribute illegal content, such as copies of copyrighted songs and movies as well as pirated software. "Warez" is a term widely used by hackers to denote illegally copied and distributed commercial software from which all copy protection has been removed. Warez often contain viruses, Trojan horses, and other malicious code and thus are very risky to download and use (legal issues notwithstanding).

A Kerberos security server provides a means by which constituents of the network (principals) can trust each other. These principals may be any hardware or software that communicates across the network. Kerberos protocol is used for local logins, remote authentication, and client/server requests. It uses a symmetric-key cryptography and a trusted third party. The principals involved in the Kerberos model are the user, the client, the key distribution center, the ticket-granting service, and the server providing the requested service.

The **SOCKS server** (socket server) is a networking-proxy protocol that enables full access across the SOCKS server from one host to another without requiring direct IP reachability.

Load-balancing servers distribute HTTP requests over multiple Web servers, allowing organizations to increase the capacity of their Web site by transparently adding additional servers. Load balancers act as virtual servers, receiving all HTTP requests to the Web site. These requests are forwarded, based on the load balancer's policy, to one of the servers that hosts the Web site. The load balancer's policy attempts to ensure that each server receives a similar number of requests. Many load balancers are capable of monitoring the servers and compensating if one server becomes unavailable.

WHAT IS SERVER LOAD BALANCING AND HOW IS IT RELATED TO CLUSTERING?

Server load balancing refers to fine-tuning a computer system, network, or disk subsystem in order to more evenly distribute the data and/or processing across available resources. The load balancing occurs when network traffic is distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. It increases server availability and application system availability, and could be a viable contingency measure when it is implemented among different Web sites. In this regard, the application system continues to operate as long as one or more Web sites remain operational.

Clustering means multiple servers providing the same service. It implies resilience to failure and/or some kind of load balancing between the servers. For example, in clustering, load balancing might distribute the incoming transactions evenly to all servers, or it might redirect them to the next available server.

Load balancers are often augmented by caching mechanisms. Many of the HTTP requests an organization's Web server receives are identical and return identical HTTP responses. However, when dynamic content generation is in use, these identical responses need to be regenerated each time the request is made. To alleviate this requirement and further reduce the load on individual Web servers, organizations can deploy caching servers.

Like network switches, load balancers are not specifically security appliances, but they are essential tools for maintaining the availability of a Web site. By ensuring that several individual Web servers are sharing the load, rather than placing the load on a single Web server, the organization is better able to withstand the high volume of requests used in many DoS attacks. Firewalls, switches, and routers should also be configured (when possible) to limit the amount of traffic that is passed to the Web servers, which further reduces the risk of successful DoS attacks.

(iv) Security over Web Servers

(A) Security Levels Recent attacks on Web sites have shown that computers supporting Web sites are vulnerable to attacks ranging from minor nuisances to significant service interruptions. Each organization has to decide its sensitivity to risk and how open it wants to be to the external world. When resources are limited, the cost of security incidents should be considered, and the investment in protective measures should be concentrated in areas of highest sensitivity.

Three levels of Web security techniques can be applied to Web servers. They operate in a cumulative manner, meaning that techniques in level 3 are stronger than those in level 1.

Level 1 Minimum Security

1. Upgrading software/installing patches
2. Using single purpose servers
3. Removing unnecessary applications

Level 2 Penetration Resistance

1. Installing external firewalls
2. Administering remote security
3. Restricting server scripts

4. Shielding Web server with packet filtering
5. Educating and allocating resources
6. Plus techniques listed in level 1

Level 3 Attack Detection and Mitigation

1. Applying separation of privileges principles
2. Installing hardware-based solutions
3. Installing internal firewalls
4. Installing network-based intrusion detection systems (IDSs)
5. Installing host-based IDSs
6. Plus techniques listed in level 2

Security controls over Web servers are discussed next.

Upgrading Software/Installing Patches One of the simplest and yet most effective techniques for reducing risk is the installation of the latest software upgrades and patches. Web servers should be examined frequently to determine what software needs to be updated or patched.

Using Single-Purpose Servers Organizations should run Web servers on computers dedicated exclusively to that task. A common mistake is to save money by running multiple servers on the same host. For example, it is common to run an e-mail server, Web server, and database server on the same computer. However, each server running on a host provides an attacker with avenues for attack. Each newly installed server increases the organization's reliance on that host while simultaneously decreasing the host's security. Given the decreasing cost of hardware and the increasing importance of having fast Web servers, it generally is effective to buy a dedicated host for each Web server. Also, in situations where a Web server constantly interacts with a database, it is best to use two separate hosts.

Removing Unnecessary Applications Privileged software is defined as software that runs with administrator privileges or that receives packets from the network. All privileged software not specifically required by the Web server should be removed.

OSs often run a variety of privilege programs by default. System administrators may not even be aware that these programs exist. Each privileged program provides another avenue by which an attacker can compromise a Web server. It is therefore crucial that Web servers are purged of unnecessary programs. For greater security and because it is often difficult to identify what software is privileged, many system administrators remove all software not needed by a Web server.

Installing External Firewalls Install public Web servers outside of an organization's firewall. In this configuration, the firewall prevents the Web server from sending packets into an organization's network. If attackers on the Internet penetrate the external Web server, they have no more access to the organization's internal network than they had before. If a Web server is inside the organization's firewall and is penetrated by attackers on the Internet, the attackers can use the Web server as a launching point for attacks on internal systems. Thus, these attacks completely bypass the security provided by the firewall.

Administering Remote Security Since it is often inconvenient to administer a host from the physical console, system administrators often install software on Web servers to allow remote administration. From a security perspective, this practice is dangerous and should be minimized or eliminated. In order to increase security where this practice is necessary:

- Encrypt remote administration traffic such that attackers monitoring network traffic cannot obtain passwords or inject malicious commands into conversation.
- Use packet filtering to allow remote administration only from a designated set of hosts.
- Maintain this designated set of hosts at a higher degree of security than normal hosts.
- Do not use packet filtering as a replacement for encryption because attackers can spoof IP addresses. With IP spoofing, attackers lie about their location by sending messages from an IP address other than their own.

Restricting Server Scripts Most Web sites contain scripts (small programs) created locally by Web site developers. A Web server runs these scripts when a user requests a particular page. Attackers can use these scripts to penetrate Web sites by finding and exercising flaws in the code. Scripts must be carefully written with security in mind, and system administrators should inspect them before placing them on a Web site. Do not allow scripts to run arbitrary commands on a system or to launch insecure or nonpatched programs. Scripts should restrain users to doing a small set of well-defined tasks. They should carefully restrict the size of input parameters so that an attacker cannot give a script more data than it expects. If an attacker is allowed to do this, a system can often be penetrated using a technique called buffer overflow. With a buffer overflow attack, an attacker convinces a Web server to run arbitrary code by giving it more information than it expected to receive. Run scripts with nonadministrator privileges to prevent an attacker from compromising the entire Web server in the event that a script contains flaws.

Shielding Web Server with Packet Filtering A router set up to separate a Web server from the rest of the network can shield a Web server from many attacks. It can thwart attacks before they reach the Web server by dropping all packets that do not access valid Web server services. Typically, the router should drop all network packets that do not go either to the Web server or to the remote administration server. For additional security, only allow a preapproved list of hosts to send traffic to a Web server's remote administration server. This way, an attacker can compromise a Web server only by using the remote administration server via a restricted set of network paths. The filtering router shield offers protection similar to that of removing all unneeded software from a host because it prevents an attacker from requesting certain vulnerable services. Be aware that setting up a router with many filtering rules may noticeably slow its ability to forward packets.

Educating and Allocating Resources Attackers are able to penetrate most Web servers because system administrators are either not knowledgeable about Web server security or do not take the time to properly secure the system. Web site administrators must be trained about Web server security techniques and rewarded for spending time securing the sites.

Applying Separation of Privileges Principles Regardless of the security measures established for a Web server, penetration may still occur. If this happens, it is important to limit the attacker's actions on the penetrated host. Separation of privileges is a key concept for restricting actions once a part of the host is penetrated. To establish such control, partition the various host resources among a set of user accounts. An attacker who penetrates some software will then be limited to acting within that single user account instead of having control over the entire system. For

example, a Web server can run as one user, but another user can own the Web pages, with the Web server given read-only access. Then, if attackers penetrate the Web server, they cannot change the Web pages owned by other users. Likewise, IDS can run as another user to protect it from being modified by an attacker penetrating the Web server user. For the best security, run the Web server process as a user that has write privilege only in a few privately owned temporary directories. This requires storing the Web server software as read-only under one user but running it as a different user.

Installing Hardware-Based Solutions Hardware can implement separation-of-privilege concepts with a greater degree of security than software because hardware is not as easily modified as software. With software implementation, if the underlying OS is penetrated, the attacker has complete control of all files on a Web server. Using read-only external hard disk or CD-ROMs, Web pages and even critical software can be stored in a way that an attacker cannot modify the files. The usual configuration is for Web servers to have a read-write port so that the Web pages can be updated. Note that an attacker who penetrates a protected Web server can still copy data, change the copied data, and serve up the changed pages.

Installing Internal Firewalls Modern Web servers often serve as front ends to complex and possibly distributed applications. In this situation, a Web server often communicates with several other hosts, each of which contains particular data or performs particular computations. It is tempting to locate these computers inside an organization's firewall for ease of maintenance and to protect these important computers. However, if an attacker can compromise a Web server, these back-end systems may be penetrated using the Web server as a launching point. Instead, it is a good idea to separate Web server back-end systems from the rest of the organization's networks using an internal firewall. Then penetration of the Web server and subsequently the Web server's back-end systems does not provide access to the rest of the organization's networks.

Installing Network-Based Intrusion Detection Systems Despite all attempts to patch a Web server and to configure it securely, vulnerability may still exist. Also, the Web server may be perfectly secure, but an attacker may cleverly overwhelm the host's services such that it ceases to operate. In this kind of environment, it is important to know when your Web server has been compromised or shut down so that service can be quickly restored. Network-based IDS monitor network traffic to determine whether a Web server is under attack or has been compromised or disabled. Modern IDS have the ability to launch a limited response to attacks or notify system administrators via e-mail, pagers, or messages on a security console. Typical automated responses include killing network connections and blocking IP addresses.

Installing Host-Based Intrusion Detection Systems Host-based IDS reside on a Web server. Thus, they are better positioned to determine the state of the Web server than a network-based IDS. They provide the same benefits as network-based IDS and in some circumstances can better detect attacks since they have finer-grained access to the Web server's state. However, some drawbacks exist. An attacker penetrating a Web server can disable a host-based IDS, thereby preventing it from issuing a warning. In addition, remote DoS attacks often disable host-based IDS while disabling the Web server. Remote DoS attacks enable an attacker to remotely shut down a Web server without actually penetrating it. Thus, host-based IDS are useful, but they should be used in conjunction with the typically more secure network-based IDS.

(B) Limitations of Techniques to Secure Web Servers Today's software is not 100% proven secure, and applications of standard Web security techniques cannot guarantee that a Web server will be impenetrable. A Web server should use its stated Web server security techniques in addition to

using trustworthy software. "Trustworthy" means software that can be assessed by studying past vulnerabilities, using software specifically created with security as the principal goal, and using software evaluated by trusted third parties.

Three issues can be raised here with Web servers:

1. Some level of assurance in software can be gained by looking at past vulnerabilities discovered in different Web server software. The number of past vulnerabilities is an indicator of future vulnerabilities and also reflects how well the software was crafted. Trustworthiness is directly related to the quality of the software product. A poorly crafted product built explicitly to meet security needs remains a poorly crafted product and therefore is not trustworthy.
2. Some companies specialize in creating very secure Web server software, and some boast that no vulnerabilities have ever been discovered. Users have to balance a vendor's security claims against any security-performance trade-offs that have been made.
3. A way to gain a level of assurance in software is to use evaluated and validated software. Many private sector organizations perform third-party evaluation of commercial products in order to verify a particular level of security.

(C) Security Testing Web Servers Periodic security testing of public Web servers is critical. Without periodic testing, there is no assurance that current protective measures are working or that the security patch applied by the Web server administrator is functioning as advertised. Although a variety of security testing techniques exists, vulnerability scanning is the most common. Vulnerability scanning assists a Web server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective. Penetration testing is also used, but it is used less frequently and usually only as part of an overall penetration test of the organization's network.

(D) Remotely Administering a Web Server It is strongly recommended that remote administration and remote updating of content for a Web server be allowed only after careful consideration of the risks. The most secure configuration is to disallow any remote administration or content updates. However, that might not be viable for all organizations. The risk of enabling remote administration or content updates varies considerably depending on the location of the Web server on the network. For a Web server that is located behind a firewall, remote administration or content updating can be implemented relatively securely from the internal network but not without added risk. Remote administration or content updating generally should not be allowed from a host located outside the organization's network unless it is performed from an organization-controlled computer through the organization's remote access solution, such as a VPN.

If an organization determines that it is necessary to remotely administer or update content on a Web server, following the next steps should ensure that content is implemented in as secure a manner as possible:

- Use a strong authentication mechanism (e.g., public/private key pair and two-factor authentication).
- Restrict which hosts can be used to remotely administer or update content on the Web server.
  - Restrict by authorized users.
  - Restrict by IP address (not hostname).

  - Restrict to hosts on the internal network or those using the organization's enterprise remote access solution.
- Use secure protocols that can provide encryption of both passwords and data (e.g., SSH and HTTPS); do not use less secure protocols (e.g., TELNET, FTP, NFS, and HTTP) unless absolutely required and tunneled over an encrypted protocol, such as SSH, Secure Sockets Layer (SSL), or IPsec.
- Enforce the concept of least privilege on remote administration and content updating (e.g., attempt to minimize the access rights for the remote administration/update accounts).
- Do not allow remote administration from the Internet through the firewall unless accomplished via strong mechanisms, such as VPNs.
- Change any default accounts or passwords for the remote administration utility or application.
- Do not mount any file shares on the internal network from the Web server or vice versa.

(c) Database Systems and Cloud Computing Systems

In this section, database management system (DBMS) software, including its advantages and disadvantages; database design approaches; database checkpoints; database compression techniques; database reorganization; database restructuring; database performance monitoring; database utility programs; data dictionary systems software; data warehouses; data marts; data mining; virtual databases; online analytical processing; and SQL are discussed.

(i) Database Management Systems Software

A database contains facts and figures on various types of information such as sales, costs, and personnel. These files are collectively called the firm's database. A database is a collection of related data about an organization, intended for sharing of this data by multiple users. The DBMS is comprised of software, hardware, and procedures. It acts as a software controller enabling different application systems to access large number of distinct data records stored on direct access storage devices (e.g., disk).

The DBMS should be compatible with the OS environment as it handles complex data structures. Unauthorized access to data elements is a major concern in a database system due to concentration of data. The DBMS helps in providing users an interface with the application system through increased accessibility and flexibility by means of data views.

Advantages (objectives) of a DBMS are are listed next. A DBMS provides:

- Minimum data redundancy resulting in data consistency.
- Data independence from application programs except during computer processing.
- Consistent and quality information for decision-making purposes.
- Adequate security and integrity controls.
- Shared access to data.
- A single storage location for each data item.
- Built-in backup and recovery procedures.

In addition, a DBMS:

- Facilitates uniform development and maintenance of application systems.
- Ensures that all applicable standards (e.g., documentation, data naming, data formats) are observed in the representation of the data.
- Improves program maintenance due to separation of data from programs.
- Separates file management tasks from application programs.
- Programs access data according to predefined subschema.

Disadvantages of a DBMS are that it:

- Can be expensive to acquire, operate, and maintain.
- Requires additional main memory.
- Requires additional disk storage.
- Requires knowledgeable and technically skilled staff (e.g., database administrator and data administrator).
- Results in additional system overhead, thereby slowing down the system response time.
- Needs additional CPU processing time.
- Requires sophisticated and efficient security mechanisms.
- Is difficult to enforce security protection policies.

Redundancy of data is sometimes necessary when high system performance and high data availability are required. The trade-off here is the cost of collecting and maintaining the redundant data and the system overhead it requires to process the data. Another concern is synchronization of data updates in terms of timing and sequence. Ideally, the synchronization should be done at the system level rather than the application level.

A DBMS understands the structure of the data and provides a language for defining and manipulating stored data. The primary functions of the DBMS are to store data and to provide operations on the database. The operations usually include create, delete, update, and search of data. Most DBMS products require extensive file backup and recovery procedures and require more processing time.

Some essential features supported by most DBMSs are listed next.

- **Persistence.** Persistence is the property wherein the state of the database survives the execution of a process in order to be reused later in another process.
- **Data sharing.** Data sharing is the property that permits simultaneous use of the database by multiple users. A DBMS that permits sharing must provide some **concurrency control** (locking) mechanism that prevents users from executing inconsistent actions on the database.
- **Recovery. "**Recovery" refers to the capability of the DBMS to return its data to a consistent and coherent state after a hardware or software failure.
- **Database language.** The database language permits external access to the DBMS. The database language may include the Data Definition Language (DDL), the Data Manipulation

Language (DML), the Data Control Language (DCL), and an ad hoc query language. The DDL is used to define the database schema and subschema. The DML is used to examine and manipulate contents of the database. The DCL is used to specify parameters needed to define the internal organization of the database, such as indexes, buffer size. Ad hoc query language is provided for interactive specification of queries.

- **Security and integrity.** Security and authorization control, integrity checking, utility programs, backup/archiving, versioning, and view definition are other features of most DBMS. Integrity checking involves two types: semantic and referential. **Semantic integrity** refers to the declaration of semantic and structural integrity rules (e.g., typing constraints, values of domain constraints, and uniqueness constraints) and the enforcement of these rules. Semantic integrity rules may be automatically enforced at program run time, at compile time, or may be performed only when a message is sent. **Referential integrity** means that no record may contain a reference to the primary key of a nonexisting record. Cascading of deletes, one of the features of referential integrity checking, occurs when a record is deleted and all other referenced records are automatically deleted.

(ii) Database Design Approaches

User requirements are specified to the conceptual model first, which represents "user views" of the database. When the conceptual model is presented to the DBMS, it becomes a logical model, external model, or schema/subschema. The type of DBMS is not a factor in designing a conceptual model, but the design of a logical model is dependent on the type of DBMS to be used. This means that the conceptual model is, or should be, independent of a DBMS.

Next the logical model is converted to a physical model in terms of physical storage media, such as magnetic disks, tapes, and disk arrays. The physical model, which is also called an internal model, considers the type of access methods needed, the type of indexing techniques required, and the data distribution methods available.

SCHEMAS/SUBSCHEMAS

- A logical view of an entire database is called a schema. Schemas may be external, conceptual, or internal. A synonym for the word "schema" is "view."
- A subschema is a part of schema. In other words, a schema is made up of one or more subschemas.
- A logical data model presents a view of data.

Logical database design is the process of determining an information system structure that is independent of software or hardware considerations. It produces logical data structures consisting of a number of entities connected by one-to-one or one-to-many relationships, subject to appropriate integrity checking. The objective is to improve the effectiveness of an information system by maximizing the accuracy, consistency, integrity, security, and completeness of the database.

Physical database design is the implementation of a logical design in a particular computer system environment. It deals with retrieval and update workloads for the system and the parameters required (i.e., average time required for random/sequential access to a track, length of a track, and disk cylinder sizes) for the hardware environment. The objective is to improve the performance of the information system by minimizing the data entry time, data retrieval time, data update time, data query time, and storage space and costs.

For large, logically complex databases, physical design is an extremely difficult task. Typically, an enormous number of alternatives must be explored in searching for a good physical design. Often optimal or near-optimal designs cannot be discovered, resulting in the creation of inefficient and costly databases. Suggested action steps required in a physical database design are listed next.

- Analyze workload complexity and characteristics.
- Translate the relationships specified in the logical data structures into physical records and hardware devices, and determine their relationships. This includes consideration of symbolic and direct pointers. **Symbolic pointers** contain the logical identifier of the other. **Direct pointers** contain the physical address of the other. Both pointers can coexist.
- Fine-tune the design by determining the initial record loading factors, record segmentations, record and file indexes, primary and secondary access methods, file block sizes, and secondary memory management for overflow handling.

Exhibit 6.9 depicts the relationships among conceptual, logical, and physical models.

EXHIBIT 6.9 Relationships among Database Models

Prior to developing a full-scale database, a prototype may be undertaken to finalize user/technical requirements of the application system. Later, the prototype can be merged into normal system design phase for security, controls, recovery, and performance considerations.

Another way of looking at the database models is from the design focus and features of the database itself. Exhibit 6.10 list features of a physical data model and a logical data model.

Physical data model	Logical data model
Concerned with physical storage of data (internal schema)	Concerned with user-oriented data views (external schema)
Concerned with the entities for which data are collected	Concerned with entities for which data are collected
Describes how the data are arranged in the defined storage media (e.g., disk) from program and programmer viewpoints	Describes how the data can be viewed by the designated end user
Physical in nature in the sense that it describes the way data are physically located in the database	Conceptual in nature (conceptual schema) in the sense that it describes the overall logical view of the database

EXHIBIT 6.10 Features of Physical and Logical data Models

A data model describes relationships between the data elements and is used as a tool to represent the conceptual organization of data. A relationship within a data model can be one to one (e.g., between patient and bed in a hospital environment; at any given time, one bed is assigned to one patient), one to many (e.g., between hospital room and patients; one hospital room accommodates more than one patient), and many to many (e.g., between patient and surgeon; one surgeon may attend to many patients, and a patient may be attended by more than one surgeon). A data model can be considered as consisting of three components.

1. **Data structure.** The basic building blocks describing the way data are organized
2. **Operators.** The set of functions that can be used to act on the data structures
3. **Integrity rules.** The valid states in which the data stored in the database may exist

The primary purpose of any data model is to provide a formal means of representing information and a formal means of manipulating the representation. A good data model can help describe and model the application effectively. A DBMS uses one or more data models, as described.

DATA MODEL TYPES

- Relational
- Hierarchical
- Network
- Inverted file
- Object
- Distributed

(A) Relational Data Model The relational data model (e.g., DB2) consists of **columns**, equal to data fields in a conventional file, and **rows**, equal to data records in a conventional file, represented in a **table**. Data are stored in tables with keys or indexes outside the program. For example, in a hospital environment, a patient table may consist of columns (patient number, name, and address) and the values in the column (patient number, 1234; patient name, John Jones; patient address, 100 Main Street, Any Town, U.S.A.) are represented in rows.

The columns of the table are called attributes while the rows are called tuples. A set of actual values an attribute may take are drawn from a domain. The primary key to the patient table is patient number. The properties of a relational data model are described next.

- All "key" values are defined.
- Duplicate rows do not exist.
- Column order is not significant.
- Row order is not significant.

Some major **advantages** of a relational model are its simplicity in use and true data independence from data storage structures and access methods. Some major **disadvantages** are low system performance and operational efficiency compared to other data models.

(B) Hierarchical Data Model From a comparison point of view, the hierarchical data model (e.g., IP Multimedia Subsystem [IMS]) can be related to a family **tree concept**, where the parents can have no children, one child, or more than one child. Similarly, a tree is composed of a number of branches or nodes. A number of trees or data records form a database. Every branch has a number of leaves or data fields. Hence, a hierarchical tree structure consists of nodes and branches. The highest node is called a "root" (parent—level 1). and its every occurrence begins a logical database record. The dependent nodes are at the lower levels (children—level 2, 3 . . .).

The properties of a hierarchical data model are described next.

- A model always starts with a root node.
- A parent node must have at least one dependent node.
- Every node except the root must be accessed through its parent node.
- Except at level 1, the root node, the dependent node can be added horizontally as well as vertically with no limitation.
- There can be a number of occurrences of each node at each level.
- Every node occurring at level 2 must be connected with one and only one node occurring at level 1, and is repeated down.

Some major **advantages** of a hierarchical data model are its proven performance, simplicity, ease of use, and reduction of data dependency. Some major **disadvantages** are that addition and deletion of parent/children nodes can become complex and deletion of the parent results in the deletion of the children.

(C) Network Data Model The network data model (e.g., IDMS/R) is depicted using blocks and arrows. A block represents a record type or an entity. Each record type, in turn, is composed of zero, one, or more data elements/fields or attributes. An arrow linking two blocks shows the relationship between two record types. A network database consists of a number of areas. An area contains records, which in turn contain data elements or fields. A set, which is a grouping of records, may reside in an area or span a number of areas. Each area can have its own unique physical attributes. Areas can be operated independently of, or in conjunction with, other areas.

Exhibit 6.11 depicts the network data model, where a patient is described as an owner record type and surgery is denoted as member record type in the set type patient-has-surgery.

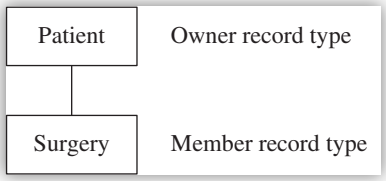


EXHIBIT 6.11 Network Model

The properties of a network data model are described next.

- A set is composed of related records.
- There is only a single "owner" in a set.
- There may be zero, one, or many members in a set.

Some major **advantages** of a network data model are its proven performance and the accommodation of many-to-many relationships that occur quite frequently in real life. Some major **disadvantages** are its complexity in programming and loss of data independence during database reorganization and when sets are removed.

(D) Inverted File Data Model In the inverted file data model (e.g., Adaptable DAta BAse System [ADABAS]), each entity is represented by a file. Each record in the file represents an occurrence

of the entity. Each attribute becomes data field or element in the file. Data fields are inverted to allow efficient access to individual files. To accomplish this, an index file is created containing all the values taken by the inverted field and pointers to all records in the file.

Some major **advantages** of the inverted file data model are its simplicity, data independence, and ease of adding new files and fields. Some major **disadvantages** are difficulty in synchronizing changes between database records/fields and index file.

(E) Object Data Model The object data model is developed by combining the special nature of object-oriented programming languages (e.g., Lisp, C++) with DBMS. Objects, classes, and inheritance form the basis for the structural aspects of the object data model. Objects are basic entities that have data structures and operations. Every object has an object ID that is a unique, system-provided identifier. Classes describe generic object types. All objects are members of a class. Classes are related through inheritance. Classes can be related to each other by superclass or subclass relationships, similar to entity-relationship-attribute model, to form class hierarchies. Class definitions are the mechanism for specifying the database schema for an application. For example, the class PERSON has an attribute SPOUSE whose data type is also PERSON.

Object DBMS also supports data sharing, provides concurrency controls and system recovery, and handles cooperative transaction processing and data versioning. Engineering applications such as computer-aided design systems, office information systems, and artificial intelligence (knowledge-based) systems require the use of cooperative transaction processing and data versioning techniques.

Version management is a facility for tracking and recording changes made to data over time through the history of design changes. The version management system tracks version successors and predecessors. When objects constituting a portion of the design are retrieved, the system must ensure that versions of these objects are consistent and compatible. Some **advantages** of the object data model are system development efficiency and handling of complex data structures. Some **disadvantages** include new technology and new risks, which requires training and learning curves.

(F) Distributed Data Model The distributed database model can be thought of as having many network nodes and access paths between the central and local computers and within the local computer sites. Database security becomes a major issue in a truly distributed environment, where the actual data are distributed and there are many access paths to the data from far-flung locations.

Data in a distributed database reside in more than one physical database in the network. **Location transparency**, in which the user does not need to know where data are stored, is one of the major goals of a distributed database data model. Similarly, programmers do not have to rewrite applications and can move data from one location to another, depending on need.

(iii) Database Checkpoints

A technique used to start at certain points in the execution of a program after the system fails or detects an error is called checkpoints. In the case of a backout, it is possible to go back to the last checkpoint instead of starting at the beginning of a program. Checkpoints are relatively easy to implement in batch programs and cumbersome for online programs due to concurrent processing.

A drawback of checkpoints is that they degrade system performance. The database designer needs to balance the number of checkpoints and the time interval between two checkpoints. Usually

the higher the number of checkpoints, the greater the degradation of performance, even though the easier the recovery process. If the time interval between two checkpoints is long, however, performance degradation is less but recovery is more difficult. A trade-off exists between the number of checkpoints and the time interval between two checkpoints.

Some criteria for designing and implementing checkpoints may include:

- Time interval
- Operator action
- Number of changes to the database
- Number of records written to the log tape
- Number of transactions processed

(iv) Database Compression Techniques

In some DBMSs, it is common to find unused space in the database due to the deletion of many records. This unused space widens the distance between the active database records, resulting in longer time for data retrieval. Compression or compaction techniques can be used to reduce the amount of storage space required for a given collection of data records. In addition to saving storage space, compression saves disk I/O operations. However, CPU activity will increase to decompress the data after they have been retrieved. A trade-off exists between the I/O savings and additional CPU activity. Indexes always gain from the use of a compression technique. Both pointers and data values can be compressed too.

(v) Database Reorganization

A fragmentation of space or unused space occurs as a result of a deletion of some records in the database. This could happen during initial loading or after the reloading of the database. A normal practice is to reorganize the database by:

- Copying the old database onto another device, such as disk or tape (where tape can act as a backup copy of the database).
- Reblocking the valid records.
- Reloading the valid records.
- Excluding the records marked "deleted" during this process.

Besides reclaiming unused space, reorganization can arrange the records in such a way that their physical sequence is the same or nearly the same as their logical sequence. It is also possible to arrange the records so that the more frequently accessed ones are stored on a disk, whereas the rarely accessed or less frequently accessed records are stored on tape. Other reorganization efforts could result from changing block sizes, buffer pool sizes, prime areas, and overflow areas.

(vi) Database Restructuring

Databases go through changes after their creation, usually because of usage patterns, application systems priorities, or performance requirements. New record types and new data elements may be added to the database. Access controls and database procedures may need to be changed. Implementing all of these changes is called restructuring the database at the logical and physical level.

Relatively speaking, database reorganization is a minor activity, and restructuring is a major activity. Usually reorganization does not affect the existing application systems and procedures, whereas restructuring does affect them. Normally, there are three types of changes in restructuring.

1. **Logical changes** in terms of adding or deleting data elements, combining a number of records, changing the relationship between records
2. **Physical changes** in terms of channels and disk configuration to minimize contention, adding or removing some pointers
3. **Procedural changes** in terms of backup and recovery procedures and access control security rules

(vii) Database Performance Monitoring

An important responsibility of a DBA is to monitor the performance of the database. The DBMS can consume large amounts of computer resources (i.e., memory, disk space) and can take long processing times due to design complexity. Often a performance-monitoring tool and/or utility programs are utilized to take internal readings of the database and its components. The objective is to identify performance-related problems and take corrective action as quickly as possible.

(viii) Database Utility Programs

The DBA needs uses these utility programs to make his or her work more effective and efficient:

- Load and restore routines can be used to create the initial version of the database.
- Dump and reload routines can be used to dump (unload) the database to backup storage for recovery purposes and to reload the database from such a backup copy.
- Statistical routines can be used to compute and analyze various performance statistics, such as file sizes and database values.
- Reorganization routines can be used to rearrange the data in the database to improve performance.
- Programs can be used to analyze database pointers and broken chains.
- Reconfiguring routines can be used to reconfigure the pointers in the database.
- Programs can be used to archive journal files.
- Programs can be used to initialize database files.
- Routines can be used to fix journal problems.
- Programs can be used to roll back or roll forward database updates.
- Routines can be used to expand database page size.
- Programs can be used to restructure database contents.
- Routines can be used to print and clear the log area of the data dictionary.

(ix) Data Dictionary Systems Software

A data dictionary or directory (DD) is an alphabetical listing that describes all the data elements (fields) in an application system and tells how and where they are used. It defines each

data element's characteristics, properties, and processes, including the size of the data field and record, the volume of records, the data field editing and validation rules with maximum and minimum values, the security levels or ratings, and the frequency of use and of changes of data elements.

Used properly, a DD presents a top-down structure or definition of a complex data element. The data editing and validation rules available in the data dictionary can be used to prevent the entry of inaccurate data into the system. The DD can be used as a corrective control because of its "where-used" information, which can be used to trace data backward and forward through the transaction as an audit trail.

The DD is a central repository of an organization's data elements and their relationships. The DD stores critical information, such as data sources, data formats, data usages, and data relationships. In this regard, a DD can be a database itself—storing data about data. A DD provides cross-references between groups of data elements and databases and indicates which computer programs use which databases. A DD is a tool to develop and maintain database as well as non-database application systems. Usually automated software is used to manage and control the DD. A manual DD can become inconsistent with what is actually in the system in a very short time. An automated DD supports the objectives of minimum data redundancy, maximum data consistency, and adequate data integrity and security.

The DD can be dependent on a DBMS, or it can be stand-alone. A dependent DD uses the underlying DBMS to manage and control its data, and it is a part of the DBMS. A stand-alone DD is a separate package from the DBMS package. *A DD may be active or passive with the DBMS software.* An active DD requires all data descriptions for a database defined or available at one time. A passive DD may or may not require a check for currency of data descriptions before a program is executed. Some major advantages of each approach are described next.

Advantages of an Active DD system

- Provides quick access to the data in the database
- Tracks database accesses and actions
- Provides valuable statistics for improving system performance
- Minimizes redundancy in storage of data descriptions
- Facilitates system documentation
- Improves data editing and validation controls
- Works well with database files

Advantages of a Passive DD System

- Less risk of commitment to a DBMS
- Easier to implementation
- Can describe data descriptions on a piecemeal basis
- Works well with conventional data files
- Serves as a documentation and communication tool

The major reports that can be obtained from a DD and its interface systems include these:

- Access control reports
- Audit trail reports
- Cross-reference reports
- Data elements and their relationships with their usage frequencies
- Summary, change, error, and ad hoc reports

In summary, a DD provides these benefits:

- It provides a consistent description of data as well as consistent data names for programming and data retrieval. This in turn provides consistent descriptive names and meanings.
- It shows where-used information, such as what programs used the data items, which files contain the data items, and which printed reports display the data items.
- It provides data integrity through data editing and validation routines.
- It supports elimination of data redundancy.
- It supports tracing of data item's path through several application programs.
- It describes the relationships among the entities.

(x) Data Warehouses

The purpose of a data warehouse is information retrieval and data analysis. It stores precomputed, historical, descriptive, and numerical data. It enables the process of extracting and transferring operational data into informational data and loading it into a central data store. Once loaded, users can access the warehouse through query and analysis tools. A data warehouse can be housed on a data storage computer different from production computer.

A data warehouse is a storage facility where data from heterogeneous databases are brought together so that users can make queries against the warehouse instead of against several databases. The warehouse is like a big database. Redundant and inconsistent data are removed from the databases and subsets of data are selected from the databases prior to placing them in a data warehouse. Usually summary data, correlated data, or otherwise massaged data are contained in the data warehouse.

Data integrity and security issues are equally applicable to warehouses as they are to databases. An issue is: What happens to the warehouse when the individual databases are updated? The warehouse should be updated either regularly or periodically for data synchronization.

Data modeling is an essential task for building a data warehouse along with access methods, index strategies, and query language. For example, if the data model is relational, then an SQL-based language is used. If the data model is object-oriented, an object-based language may be appropriate.

Metadata management is another critical technology for data warehousing. Metadata includes the mapping between the data sources (databases) and the warehouse. Another issue is whether the warehouse can be centralized or distributed.

DATABASE VERSUS DATA WAREHOUSE

- A database contains raw data.
- A data warehouse contains massaged (cleaned-up) data.
- Users query many points with heterogeneous databases.
- Users query only a single point with data warehouse.

(xi) Data Marts

A data mart is a subset of a data warehouse. It brings the data from TPSs to functional departments (i.e., finance, manufacturing, and HR) or business units or divisions. Data marts are scaled-down data warehouses, where targeted business information is placed into the hands of more decision makers.

DATA MART VERSUS DATA WAREHOUSE

- A data mart provides detailed data for a specific function of a business.
- A data warehouse provides summary data for the entire business.

(xii) Data Mining

Data mining can be applied to databases as well as to data warehouses. A warehouse structures the data in such a way so as to facilitate query processing. Data mining is a set of automated processes that convert the data in the warehouse into some useful information. It selects and reports information deemed significant from a data warehouse or database.

Data mining is the process of posing a series of queries to extract information from the databases. A data warehouse itself does not attempt to extract information from the data contained in the warehouse. A data mining software is required to do this.

There are several types of data mining applications, including data classifications, data sequencing, data dependencies, and deviation analysis. Data records can be grouped into clusters or classes so that patterns in the data can be found. Data sequencing can be determined from the data. Data dependencies, such as relationships or associations between the data items, can be detected. Deviation analysis can be performed on data. Fuzzy logic, neural networks, and set theory are some techniques that data mining tools use.

Data mining techniques can also be used for intrusion detection, fraud detection, and to audit databases. Data mining tools can be used to detect abnormal patterns in data, which can provide clues to fraud. A security problem can be created when a user poses queries and makes sensitive hypotheses. That is, the inference problem occurs via data mining tool. A data mining tool can be applied to see if sensitive information can be deduced from unclassified information legitimately obtained. If so, then there is an inference problem. An inference controller can be built to detect user motives and prevent the inference problem from occurring. The inference controller can be placed between the data mining tool and the database. Since data mining tools are computationally intensive, parallel processing computers are used to carry out the data mining activities.

Examples data mining applications are listed next.

- Market segmentation, where the data mining tool identifies the common characteristics of customers who buy the same products
- Customer defection, where it predicts which customers are likely to leave the company
- Fraud detection, where it identifies which transactions are most likely to be fraudulent
- Direct marketing, where it identifies which prospects are targets for mailing
- Market basket analysis, where it identifies what products or services are commonly purchased together
- Trend analysis, where it reveals the difference between a typical customer this month versus last month

DATA MINING AND DATA AUDITING

- Data mining is a user tool to select information from a data warehouse.
- Data mining is an auditing tool to detect fraud, intrusions, and security problems in a data warehouse.

(xiii) Virtual Databases

A virtual database is created when data from multiple database sources are integrated to provide a total perspective on a specific topic. The database is virtual in that such a database does not exist physically but is created on demand. For example, an auditor comparing performance of a multiplant organization can use virtual database technology to view key operating and financial ratios of each plant side by side.

(xiv) Online Analytical Processing

Online analytical processing (OLAP) programs are available to store and deliver data warehouse information from multidimensional databases (MDBs). OLAP allows users to explore corporate data from a number of different perspectives, such as product, geography, time, and salesperson.

OLAP servers and desktop tools support high-speed analysis of data involving complex relationships, such as combinations of a company's products, regions, channels of distribution, reporting units, and time periods. Access to data in MDBs can be very quick because they store the data in structures optimized for speed, and they avoid using SQL and index processing techniques. In other words, MDBs have greater retrieval speed and longer update times.

Consumer goods companies (e.g., retail) use OLAP to analyze the millions of consumer purchase records and transactions captured by electronic scanners at the checkout stand. These data are used to spot trends in purchases and to relate sales volume to store promotions (coupons) and store conditions (displays). The data in OLAP are generally aggregated giving information such as total or average sales in dollars or units. Users can examine the OLAP's hierarchical data in the time dimension, such as sales by year, by quarter, by month, by week, or by day.

(xv) Structured Query Language

The primary components of an SQL database are schemas, tables, views, parser, optimizer, executor, access rights checker, and access rights grantor or revoker. A schema describes the structure

of related tables and views. Tables hold the actual data in the database; they consist of rows and columns. Each row is a set of columns; each column is a single data element. Views are derived tables and may be composed of a subset of a table or the result of table operations (e.g., a join of different tables). A parser is a program that breaks input into smaller chunks so that a program can act upon the information.

SQL is a standard query language for relational DBMS that is also used to query and update the data managed by the DBMS. The SQL standard, which is used by most commercial DBMSs, includes specific requirements for enforcing discretionary access controls (DACs).

Basically, two types of access control policies are applied to SQL: DAC and mandatory access control (MAC).

1. **DAC** is a means by which access to objects is restricted to specific users or groups of users. The access control is discretionary in that the object's owner may pass on access privileges to other users, either directly or indirectly. Privileges are means by which SQL enforces DAC. Privileges are granted with a grant statement and are used to specify an allowable action on a specific object (e.g., to update the rows in a specific table or to a grantee). Grant, revoke, and role statements are available to allocate individual privileges. The role facility allows a DBA to create individual roles with corresponding database access requirements. An additional benefit of roles is that a user can have only one role active at a time. For example, a role would allow a user to access only payroll-related objects when working under the payroll role and only procurement-related objects when working under the purchasing role.
2. **MAC** is not supported directly in SQL. **Polyinstantiation** is frequently used with MAC database systems to control inference. MACs require support for security labels. These labels are used as the basis for access control decisions. In order to correctly label data, the system must request and receive the security level of data. Encryption and cryptographic checksums are employed to protect the security label from modification.

Aggregation is primarily a MAC problem. The aggregation problem occurs when two pieces of information, A and B, are classified at level X individually but level Y (Y higher than X) collectively. To limit aggregation, access should be limited as tightly as possible.

Most databases use SQL, and many have Web interfaces that may be vulnerable to typical Web attacks, such as XSS or SQL injection. The communication link between data and decision layers is the primary attack surface for SQL injection. To understand the scope of a threat surface, all segments of the database system, with an emphasis on entry points, must be examined. The cascading effect of corrupted databases due to injection into database content can impact data acquisition servers and data historians. Attackers can use automated malware kits to conduct SQL injection attacks.

Many intrusion prevention systems (IPSs) claim to thwart SQL injection attacks, but their capabilities are weak and are usually based on signatures, which hackers can easily evade. SQL injections in Web applications can be thwarted by binding variables in SQL statements. Unfortunately, many programmers still do not use the bind variables method when developing applications, so databases are left exposed to SQL injection. If not controlled, SQL can lead to slammer worm attack.

(XVI) Cloud Computing Systems

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics—on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service—three service models—cloud software as a service, cloud platform as a service, and cloud infrastructure as a service—and four deployment models—private cloud, community cloud, public cloud, and hybrid cloud.

The emergence of cloud computing promises to have far-reaching effects on the systems and networks of many organizations. Many of the features that make cloud computing attractive, however, can also be at odds with traditional security models and controls. The major issues include security and privacy of data. Next, we discuss the security downside (bad news) and the security upside (good news) of cloud computing environment.

(A) Security Downside Some of the more fundamental concerns in cloud computing are listed next.

- System complexity
- Shared multitenant environment
- Internet-facing service
- Loss of control

As with any technology, cloud computing services can be turned toward improper or illicit activities, such as botnets and cracking mechanisms, such as a Wi-Fi Protected Access (WPA) cracker.

(B) Solutions to the Security Downside The next security controls can mitigate the security downside of cloud computing environment.

- Deploy access control and intrusion detection technologies at the cloud provider, and conduct an independent assessment to verify that they are in place. Doing this includes traditional perimeter security measures in combination with the domain security controls. Traditional perimeter security includes:
  - Restricting physical access to network and devices.
  - Protecting individual components from exploitation through security patch deployment.
  - Setting as default the most secure configurations.
  - Disabling all unused ports and services.
  - Using role-based access control.
  - Monitoring audit trails.
  - Minimizing the use of privileges.
  - Using antivirus software.
  - Encrypting communications.

- Define trust boundaries between service providers and consumers to ensure that the responsibility for providing security is clear.
- Support application and data portability such that the customer can take action to change cloud service providers when needed to satisfy availability, confidentiality, and integrity requirements. Doing this includes the ability to close an account on a particular date and time and to copy data from one service provider to another.

(C) Security Upside The cloud computing paradigm provides opportunities for innovation in provisioning security service that holds the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of IT administrators and security personnel and lack the economies of scale available for larger organizations with sizable data centers. Potential areas of improvement where organizations may derive security benefits from transitioning to a public cloud computing environment are listed next.

- Staff specialization
- Platform strength
- Resource availability
- Backup and recovery
- Mobile endpoints
- Data concentration
- Data center oriented (e.g., redirecting e-mail records to a cloud provide via mail exchange records to discover widespread spam, phishing, and malware campaigns and to carry out remedial actions, such as quarantining suspect messages and content)
- Cloud oriented (e.g., reverse proxy products are available that enable unfettered access to a cloud environment yet maintain the data stored in that environment in encrypted form)

(D) Key Security Considerations Major security considerations in cloud computing includes the need to:

- Carefully define security and privacy requirements during the initial planning stage at the start of the SDLC.
- Determine the extent to which negotiated service agreements are required to satisfy security requirements and the alternatives of using negotiated service agreements or cloud computing deployment models, which offer greater oversight and control over security and privacy.
- Assess the extent to which the server and client-side computing environment meets organizational security and privacy requirements.
- Continue to maintain security management practices, controls, and accountability over the privacy and security of data and applications.

(E) Potential Vulnerabilities Potential vulnerabilities associated with various cloud computing service and deployment models are listed next.

- The inherent system complexity of a cloud computing environment and the dependency on the correctness of these components and the interactions among them

- The dependency on the service provider to maintain logical separation in a multitenant environment, which is not unique to the cloud computing model
- The need to ensure that the organization retains an appropriate level of controls to obtain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interests of an organization

(F) Security Requirements The goal is to ensure that a safe and secure cloud solution is available to provide a prospective IT service. The following security needs must be considered:

- Statutory compliance to laws, regulations, and organization requirements
- Data characteristics to assess which fundamental protections an application's data set requires
- Privacy and confidentiality to protect against accidental and nefarious access to information
- Integrity to ensure data are authorized, complete, and accurate
- Data controls and access policies to determine where data can be stored and who can access physical locations
- Governance to ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls, and provide the information necessary for the organization to appropriately and independently assess and monitor the efficacy of those controls

(G) Potential Security Benefits Potential security benefits of using cloud computing services are listed next.

- The ability to focus resources on areas of high concern as more general security services are assumed by the cloud provider
- Potential platform strength resulting from greater uniformity and homogeneity, and resulting improved information assurance, security response, system management, reliability, and maintainability
- Improved resource availability through scalability, redundancy, and disaster recovery capabilities; improved resilience to unanticipated service demands
- Improved backup and recovery capabilities, policies, procedures, and consistency
- Ability to leverage alternate cloud services to improve the overall security posture, including that of traditional data centers
- Reduced time-to-market metric regarding access provisioning of new applicants

(H) General and Specific Security and Privacy Issues Data processed in a public cloud computing environment and applications running in a public cloud facility can experience different security and privacy exposures than would be the case in an onsite hosted environment. For example, cloud subscribers, who are ultimately responsible for their data processed on provider's systems, must require assurances from providers that they are in compliance with the appropriate regulations.

Examples of **general security and privacy issues** in a public cloud environment include:

- Not meeting the subscriber's data protection requirements.
- Not providing encryption of data at rest in storage.

- Not knowing the strengths of the encryption algorithm.
- Not knowing the attack surface of a cloud and the likely pool of attackers.
- Not knowing the expertise level of cloud administrators.

Examples of **specific security and privacy issues** in public cloud computing environment include:

- Storing sensitive data without adequate protection due to risk of unintended data disclosure.
- Lack of subscriber awareness over where data are stored and who has or can have access, leading to privacy concerns due to the distributed nature of clouds.
- Inability to partition access rights among subscribers, providers, and administrators, thus compromising system integrity.
- Not having both logical separation and physical separation of systems required to protect a subscriber's resources due to multitenancy.
- Using a subscriber's browser as a graphical interface, account setup, and resource administration, leading to security flaws.
- Lack of proper protection of a subscriber's cryptographic keys to ensure a safe use of cryptography from inside a cloud.

(d) Functional Areas of Information Technology Operations

Data (computer) center operating environment; computer operations; change and problem management; SLAs; separation of duties in IT operations and other functions; and network management in terms of its architecture, management categories, changes, and interoperability are discussed in this section.

(i) Operating Environment

Activities include data input and output procedures, production program execution procedures, job scheduling practices, and production job turnover procedures.

(A) Data Input and Output Procedures The data control or production control function is the first line of defense in the computer center against possible delays, errors, omissions, and irregularities. This is due to the fact that many front-end activities, such as data entry, job setup, and job scheduling, are performed prior to executing production jobs for application systems. The things that data/production control staff do and how well they do them will have a great impact on subsequent activities, such as computer operations, backup and recovery, storage media management, help desk, and report delivery. Consequently, there are many potential risks and exposures in the data or production control work area.

WHAT ARE SOME EXAMPLES OF DATA CENTER OR COMPUTER OPERATIONS ATTACKS?

- **Maintenance accounts** are one of the most common methods hackers use to break into computer systems. They are accounts that still have factory-set or easily guessed passwords.
- **Diagnostic port attacks** allow hackers to access large systems through diagnostic ports meant for third-party maintenance vendors.
- **Keyboard attacks** refers to data scavenging through resources available to normal system users, which may include advanced software diagnostic tools.

- **Laboratory attacks** refers to data scavenging through the aid of what could be precise or elaborate equipment.
- **Physical piggybacking** is where an unauthorized person enters a computer center behind an authorized person. Either the door is wide open or the first person lets the second one in.

The **goal** of a data control management should be to:

- Encourage remote printing where a printer is attached to a local terminal, PC, or workstation for timely printing.
- Discourage central printing at the computer center to minimize delays and labor and print costs.
- Encourage electronic report viewing facilitated by an automated report distribution software. Electronic report viewing is not a substitute for the hard-copy report printing; rather, report printing can be done in a discretionary manner.

(B) Production Program Execution Procedures Production control activities include scheduling of jobs and controlling production job turnover procedures, among other things. Some typical activities of a computer operator include those listed next.

- Execution of production jobs and programs
- Monitoring of system resources, including the computer consoles, hardware preventive maintenance, and operational changes
- Backing up of program and data files
- Mounting/unmounting of tapes, and disks
- Recording of operational problems
- Monitoring of physical security and environmental controls
- Housekeeping activities and logging of system activities

(C) Job Scheduling Practices The operations manager has a difficult task in balancing the amount of scheduling work to do and the amount of resources with which to do it. Consequently, work must be prioritized based on user business needs. In this regard, most important considerations are peripheral devices (e.g., tape or disk drives) required, job execution time, and memory required. The least important consideration is how the operator interacts with the user. Most production jobs will have a predecessor and successor job to be run.

Job scheduling can be done either manually on paper or automatically using a computer system. Manual scheduling is slow and prone to errors if the computer center environment is complex. The decision as to whether computer job scheduling is done manually or not depends on various factors, such as

- **Single CPU or multiple CPUs.** Multiple CPUs require an automated job scheduling system.
- **Number of total jobs to be run in a time period.** The greater the total number of jobs, the greater the need for automation.

- **Number of operating shifts.** The more work shifts in operation, the greater the need for automation.
- **Number of concurrent priority-one jobs to be run.** Paper schedules will become difficult to manage as the number of concurrent priority-one jobs increases.

Usually, when a new application system is being developed, run times and other resource requirements (e.g., disk space and tape space) are estimated for each job by the system development group. Operations management then determines how best to accommodate these requirements in light of other job needs.

(D) Production Job Turnover Procedures Production problems stem from hardware failures (10%), systems software failures (20%), and applications software failures (70%). Applications software failures are usually the result of problems originating in or unaddressed by the applications software development and maintenance work area. The most prevalent causes of those failures are listed next.

- Incomplete software testing by programmers and functional end users for new application systems development work
- Inappropriate software **regression testing** by programmers for existing application systems maintenance work
- Inappropriate changes made in common program modules, such as copy members, macros
- Unreliable paper records and manual procedures in the user and information systems departments
- Lack of production/operation acceptance testing by computer operations staff
- Lack of or inadequate QA review by production scheduling and control staff
- Overall poor-quality job turnover procedures
- Inexperienced programmers, production control analysts, and computer operators

Some ways to reduce or eliminate the business risk are to automate the production turnover process and to focus on software configuration management. Online approvals and automatic transfer of programs from test to production via QA libraries or from test to production directly will dominate the automation process. A QA library (as shown in Exhibit 6.12) is a staging library where final quality reviews and production setup procedures take place. Software configuration management helps in identifying the locations and the number of computer machines needed and in determining the networks that need to be propagated with new or changed software.

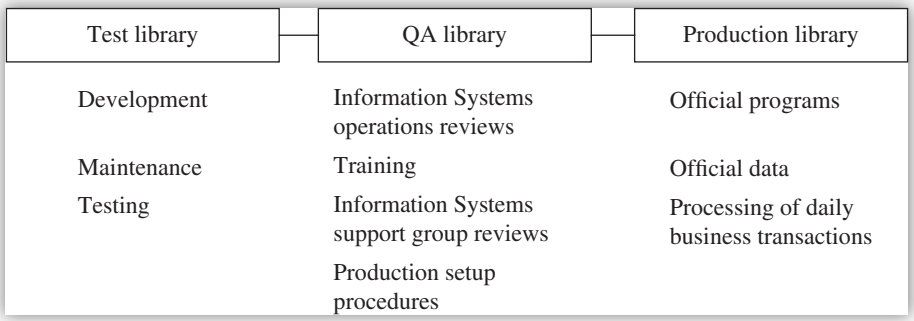


EXHIBIT 6.12 Libraries Involved in a Job Turnover Process

(ii) Computer Operations

Activities such as console operations, system commands and parameters, system backups, system backup alternatives, data file backup methods, tape handling, tape cleaning and degaussing, and preventive maintenance are a part of computer operation's work. Other activities include system logs and help-desk functions.

(A) Console Operations An important task for the computer operator is operating the system console. The OS sends questions and messages to the operator for a response. It is estimated that 90% or more of these messages are trivial in nature and do not require the operator's attention. Yet they consume valuable operator time and cause frustration to the operator due to their presentation speed. Software is available to automate the console operations and to suppress trivial messages so that the operator responds only to important questions and messages.

Computer operators should have access to system console and operator manuals, not program documentation. They should not perform run-to-run balancing procedures. The console log should contain operator commands, operator messages, and system abnormal ends, not data entry errors.

(B) System Commands and Parameters System commands and system parameters are the most significant privileged computer operations functions that should be monitored and controlled. Some examples of **system commands** and related information captured by OS console logs are listed next.

- Operator commands and operator responses to system commands
- Equipment problems and failures (tape or disk failures)
- Equipment status (active or inactive)
- Frequency of operator commands by command type or code
- Tape bypass label processing overrides
- Abnormal job terminations
- Job execution time with start and stop times
- Terminal communication problems, such as messages held
- OS abnormal ends
- Database dumps start and completion times
- Database recovery and startup messages
- Print files in queue
- Transactions up (available) or down (not available) requests from users
- Communication management system start and finish times, which are needed to backup databases
- Job reruns and their times
- System starts and restarts (e.g., initial program load, cold start/restart, warm start, stop restart, deferred restart, and checkpoint restart)

System parameters define the system configuration, determine what features and services are provided, and describe how they will be processed and accessed. Configuration files, system

files, or files with sensitive information must be retained in a secure location due to their access restrictions. Some examples of where parameters are used are listed next.

- In a computer-based application sort operation, relevant parameters include number of records sorted, size of records sorted, number of sort keys, and size of sort keys.
- In a computer-based application, resources consumed, relevant parameters include CPU time, I/O usage, memory allocated and/or used, unit device activity and volume, and number of characters transmitted/received.
- In a private branch exchange system (PBX), relevant system parameters include phone extension numbers, class of service codes, types of trunks, and trunk groups to meet the customers' needs.
- In call-processing software, relevant parameters checked include data rate, parity bit, and clock configuration for synchronous terminals.
- In network resource management, relevant parameters for all types of communications include peak rate, average rate, peak rate duration, source type, and traffic volume.
- In security-related information, critical security parameters include cryptographic keys and authentication data such as passwords and PINs.

There are some concerns about system parameters because they are set either by vendors or IT organizations and are subject to modification, either intentional or accidental. Consequently, parameters require proper care and protection when assigned to computer operators and administrators. Greater protection is required for parameters passed between interface systems and exit points between the OS and the other system software. When vendor software is upgraded due to new release, the old parameters need to be reviewed and updated to meet the functions of the new software. It is best to log and report these parameters for timely review and action.

There are also some concerns about prohibited ports, protocols, and services. To address these issues, the information systems security management should review functions and services provided by internal information systems or individual components of information systems to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol (VoIP), Instant Messaging (IM), auto-execute, and file sharing). Management should consider disabling unused or unnecessary physical and logical ports and protocols (e.g., USB, FTP, Internet Protocol Version 6 [IPv6], HTTP) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Management can utilize network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls, and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

(C) System Backups Hardware failures, disk crashes, power outages, software failures, and other disruptions are normal in computer center operation. Periodic system backups provide the ability to recover and restart from a failure or disaster and prevent the destruction of information. *System backups include backing up of operational application programs, data files, databases, systems software products, system development programs, utility programs, and others.*

Timely system backups help in reconstructing any damaged files (recovery) and resuming computer program execution (restart). For example, online and real-time systems and database systems require duplicate backup arrangements and extensive backup and recovery and restart procedures.

For online systems, restart procedures identify transactions that were lost when the online process failed. Another related backup mechanism is *checkpoints* that allow program restarts. Checkpoints are most effective for batch (sequential processing), online data entry, and batch update processing and multiprogramming and are least effective for online real-time systems due to their instant access and updates. Checkpoints are needed to recover from hardware failures and are usually applicable to sequential files, direct (random) access files, and tape or disk files. Exhibit 6.13 compares the backup requirements between online and batch systems.

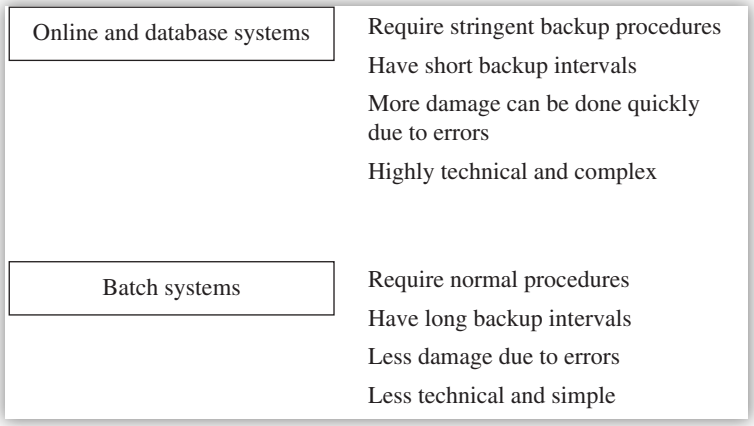


EXHIBIT 6.13 Backup Requirements for Online and Batch Systems

A prerequisite to the performance of timely system backups is the availability of accurate and up-to-date operations documentation (run books), which includes run-time instructions, backup schedules, and recovery/restart procedures for each application system in the production environment. The decision on how often to back up a file is dependent on cost of backup versus expected cost of failure, capability of re-creating the file without a backup, and time needed to create a copy.

(D) System Backup Alternatives System/data backups are maintained through a combination of these manual methods:

- **Full-volume backups,** which are common, involve compressing the image copy of an entire magnetic disk volume to a tape. This is also known as the brute-force approach since it takes copies of all files regardless of the need or file changes. It takes less time to back up and is less error-prone but requires more magnetic media to store and more manual intervention.

  This method is most applicable to database programs and data files due to the logical relationships between data. System recovery is achieved by restoring the database and reapplying transactions from the journal or log. Journals and logs are records of all the transactions that have been processed against a database. The log contains before-and-after images of transactions for all changes. In the event of a failure, the database is restored, and all the changes that have occurred up to the point of failure are reapplied to the database. Some databases are so large that record-level backup is performed whenever a change to the logical database record occurs.

- **Incremental backups,** a different approach, focus only on backing up data sets that have changed since the last full backup. The need for continuous, uninterrupted online system availability leaves a reduced window for full backups, which, in turn, justifies the use of incremental backups.

WHAT ARE THE THREATS AND INAPPROPRIATE ACTIVITIES IN COMPUTER OPERATIONS?

- Threats include errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, espionage, and malicious code.
- Inappropriate activities include fraud, collusion, sexual harassment, waste, abuse, and theft.

(E) Data File Backup Methods Usually tape files are backed up using a three-generation (son, father, and grandfather) concept, where each generation represents a time period (e.g., seven or five operating days). Disk files are saved for five or seven generations. Each generation can have multiple copies and be rotated between onsite and offsite. Tape files are a major obstacle to unattended computer center operation due to their labor-intensive nature.

(F) Tape Handling Tape library and tape handling operations are labor intensive, time consuming, and error-prone due to monotonous work and sheer volume of tape mount activity. The efficiency of a tape handling operation depends on many factors, including those listed next.

- Size of the tape and cartridge library
- Workload peaks and valleys
- Physical layout of the tape drive and tape library area
- Number of tape operators available
- Number of tape drives available
- Number of operating shifts per day
- Number of tape mounts that must be made per operating shift
- Technical sophistication of available hardware and software

The decision whether to use tape/cartridge or disk storage media for a data or program file (data set) should be based on a cost/benefit analysis. Some factors that should be considered are listed next.

- Size and complexity of the file (number of records and record types)
- Frequency of file usage (daily, weekly, period-end)
- Volatility of the file (number of records added, changed, and deleted)
- File access method (direct/random, sequential)
- File structure (fixed length, variable length)
- Transportability of the file (offsite storage, third-party processing, remote processing)

These guidelines, although not absolute, can be useful when deciding between tape/cartridge or disk media:

- Choose disk storage media when small size, infrequently used, and random access data sets need to be processed.

- If disk media is used, the choice is between fixed or removable disk. Fixed disk is faster and cheaper than removable disk. Removable disks can be physically secured by removing and locking them separately if such a need arises.
- Choose tape/cartridge storage media when large-size, frequently used, and sequentially processed data sets need to be processed. Tape/cartridge files are easy to transport.
- If tape/cartridge is used, the choice is between manual (human) or automated (robotics) handling.

(G) Tape Cleaning and Degaussing In addition to performing record keeping of tape and cartridge activity and taking periodic inventory of tapes/cartridges, the tape librarian must clean and recertify the reel tapes and cartridges to prolong their lives. The cleaning equipment should clean both sides of the tape/cartridge, measure the length, test for damaged tape, isolate errors, and retension the tape to industry standards. Cartridges are more reliable and hold more data than reel tapes.

The process of demagnetizing (erasing) the contents of tapes and cartridges is called **degaussing**. It is suggested that when tapes/cartridges are disposed of or no longer in use, they should be subjected to degaussing procedures, especially when they contained sensitive data. Disk files are demagnetized by overwriting three times with 0, 1, and a special character, in that order, so that sensitive information is completely deleted.

(H) Preventive Maintenance The regular practice of preventive maintenance of computer equipment and other system components will provide the assurance of continuity of computing services to end users. Here computer equipment includes the CPU, printers, terminals, and disk/tape drives. Other system components include physical channels, control units, cables, air conditioning units, uninterrupted power supply machines, and other mechanical/electrical devices.

The operations manager first needs to analyze the failure rates for each of the computer equipment and system component parts. After knowing the failure rates, the manager should determine the impact of failing equipment or a component on the completion of application system production job schedule. Component failure rates and impact analysis will allow the manager to shift the processing schedules either manually or automatically to balance the workload. Mean time between failures should be determined for each piece of computer equipment and the system components.

The output of component failure rates and impact analysis can be used to establish system availability objectives and service levels between hardware vendors and computer operations management. Here are some examples of system availability objectives:

- The CPU should be available for 99% of all scheduled production time.
- Disk/tape drives should be available for 98% of scheduled time
- Terminals and printers should be available for 95% of the time.

A preventive maintenance log helps operations managers and hardware vendors in tracking problems. The log can be maintained by computer operators or supervisors.

(I) System Logs Another important task performed by the computer operations staff is logging and monitoring various systems activities. A transaction log is a processing control that provides an

audit trail and is good for online systems. It is useful for file reconstruction and error tracing if errors occur in updating online files. Here we focus on 10 types of logs and their contents.

1. An **application transaction log** includes: transaction code; record type; date and time stamp; user ID or department; terminal ID; transaction amount; transaction activity (add, inquire, delete); and application-specific information.

SYSTEM LOGGING FACILITIES

System logging facilities collect vast amounts of data by design. The key is to determine what types of data to collect and how much.

2. A **database log** includes: Before images (helps in database roll-back); after images (helps in database roll-forward); I/O file information; access errors; date and time stamp; transaction type and ID; terminal ID; user ID or department; programs used or called; access authorizations; input messages; output messages (transaction was complete or not); and list of data blocks read.
3. An **OS (console) log** includes: job ID; date and time stamp; job run times (start and finish times); input and output files used; programs used; disk and tape/cartridge devices used; job completion codes (including abnormal ends and successful ends); computer operator interventions; system diagnostic messages; and file backup times and recovery/restore times.
4. A **telecommunications log** includes: originating terminal ID; transmission line ID; job ID; communication port ID; date and time stamp; type of application; session type (e.g., bound or not bound); session start and finish times; transmission error messages; user authorization code; transaction ID; message ID; control totals; port/node ID; dial-back telephone number; and messages awaiting transmission.
5. An **access control security log** includes: user ID; terminal ID; date and time stamp; transaction ID; data sets used; job ID; sign-on ID modifications; access rule modifications; type of security violations (read when not authorized); unauthorized access attempts and messages; invalid attempts of password; and last activity date. The security system can be found to operate on warning, log, or abort mode.
6. A **job accounting log** includes: job name and ID; job run time with start and finish times; date and time stamps; input and output files used; programs used; user type information (user ID, accounting code, division ID); job completion codes; control totals based on number of records or dollars; input and output devices used; CPU time consumed for the job; and other resource usage data.
7. A **problem (help desk) management log** includes: a problem number; problem type and description; problem reported time/date; problem source (i.e., failing software, hardware device, network component); name, department, phone number of person reporting the problem; problem resolution status code (i.e., open, closed, transferred) with action dates; name of the (help desk) person who took the call; name of the person who worked on the problem; and description of final response/resolution of the problem and feedback to the person who reported the problem.
8. A **change management log** includes: a change number; change type and description; change requestor name and time/date; change source (i.e., failing software or hardware

device problem); change status code (i.e., open, closed, deferred) with action dates; name of the person who worked on the change; and description of final outcome of the change and sign-off by the person affected by the change.

9. A **hardware preventive maintenance log** includes: date/time that a hardware device failed; serial number and location of the hardware device failed; time when service request was made; time when service arrived; time when problem was fixed; description of cause of problem; nature of repair and cost; and warranty period.
10. A **system management log** includes: date and time stamps; data sets accessed, renamed, and scratched; system paging activity; job CPU times; job/step termination record; data lost record; jobs using tape bypass label processing; and remote user access.

(J) Help Desk Functions In order to provide quality and timely support and service to end users, many computer centers are establishing an end-user support function. This includes an information center, help desk, 24-hour hotline services, telephone voice response system, and automated problem and change management systems.

A help desk function can implement telephone hotline services so that end users can call in with their problems and ask pertinent questions. These problems could be related to problems as diverse as printer/terminal operations, OS malfunctions, telecommunications software incompatibilities, or applications software glitches. The help desk person will try to solve a problem; if he or she cannot, the person will route the problem to the right person, it is hoped. Problem logging, routing, and escalation procedures are needed to resolve problems in a timely and proper manner.

Voice response systems could supplement the help desk function in terms of directing the end user to the appropriate person. Other developments include the implementation of expert systems that aid help desk staff diagnose and resolve problems.

(iii) Change and Problem Management

Installation of a change/problem management system or service is another end-user service and support tool where problems and changes are logged, tracked, reported, resolved, and implemented.

The goals of the computer center operations management should be to:

- Stabilize the production environment and limit negative impact (system outages, errors, backouts, and downtime) due to changes or problems.
- Maintain the integrity and security of all program modules, hardware devices, and network components within the production environment.
- Prioritize those changes that are critical to business function versus those changes that can be deferred.
- Coordinate all problems and changes in a controlled and coordinated manner.
- Promote a proactive mode of computer operations instead of a reactive one.

Often incorrectly implemented changes cause problems. There should be a cross-reference between a change and a problem caused by a change. To some extent, integrity, liability, and availability of computer systems depend on the way problems and changes are managed, controlled, and secured. Problem management is critical to online processing due to the high visibility of

problems to end users. Changes can be classified into standard change requests, mandatory change requests, and emergency change requests, so that priorities can be established and resources can be allocated accordingly.

Changes can arise from:

- Changes in applications and systems software.
- Changes in procedures (automated or manual).
- Installation of new software products and equipment.
- Introduction of new work tools and techniques.
- Changes in equipment and people.
- Changes in organizational structure.
- Changes in business requirements.

Problems can result from:

- OS failures.
- Application program failures.
- Processor (CPU or front-end) failures.
- Computer terminal failures.
- Telecommunication line and equipment failures.
- Printer failures.
- PC or workstation failures.
- Change control failures.
- Failed changes.

(iv) Service-Level Management

Service-level management is an effective way for the computer center management to improve quality of computing services to system users. The computer center management must define a set of user service levels or service objectives that describe application systems, volume of transactions, processing windows, online system response times, and batch job turnaround times. Without defined service levels to monitor against actual performance determined in the resource utilization function, a computer system's capacity limit is difficult to identify. Without service levels, the computer center management will consider that the capacity of a computer is near its limits when the users begin to complain about computer performance.

By monitoring performance against service levels, the computer center management can identify approaching problems in meeting service objectives. In order to achieve these goals, computer center management needs to develop service-level objectives for internal use. Some examples of areas requiring service level objectives are listed next.

- System capacity during peak hours in terms of average CPU busy, average demand paging rate, and maximum channel busy

- Number of online users, number of online transactions per minute, and number of batch jobs per hour
- Online system average response time in seconds by application
- Percentage of time the online system is available
- Turnaround time for test and production batch jobs processed under each job class by application
- Number of job reruns and time lost due to job reruns
- Number of abnormal terminations by application program per operating shift

Where applicable, maximum and minimum numbers (range) should be identified for each of these objectives. The rationale behind developing service-level objectives internally first is that they provide a basis for negotiating service-level agreements (SLAs) with the user community.

After developing service-level objectives internally, the computer center management is ready to negotiate with each business user to develop formal SLAs. Some examples of SLAs are listed next.

- Average response times for each online application system
- Turnaround times for each batch job by application system
- System availability time (system up-time) by each application system
- Accuracy limits in terms of number of errors by cause for each application system
- Number of job reruns by each application system
- Number of transactions to be processed during peak hours in each application system
- Number of production problems by application system per week
- Computer report delivery times by application system
- Plan for reporting service-level problems
- Action priorities if services cannot be delivered
- Scheduled meetings to discuss service levels between end users and computer center management

It is important to remember that these SLAs are not static. They require periodic adjustments and refinements, such as at least once a year or preferably at the time of renegotiation of the agreement with customers (users).

(v) Separation of Duties in IT Operations and Other Functions

The objective of separation of duties is to ensure that no one person has complete control over a transaction throughout its initiation, authorization, recording, processing, and reporting. A similar concept applies equally to any operation performed by IT or user department employees. The rationale is to minimize incompatible functions, which are not conducive to good internal control structure.

The degree of separation of duties depends on the job level. More separation of duties is practiced at the lower levels of the organization than at the higher levels. The rationale is that someone at higher levels needs to be in charge of many functions, activities, and operations.

At a minimum, the listed functions in the IT environment should be separated from each other at lower levels.

Incompatible IT Functions

- Data entry and production job scheduling
- Computer operations and applications programming
- Computer operations and systems programming
- Application programming and systems programming
- Systems programming and data security administration
- Data security administration and DA (includes database administration)
- Data administration and quality assurance
- Database administration and applications programming
- Telecommunication network and computer operations
- Quality assurance and applications development/maintenance
- Quality assurance and systems programming

Compatible IT Functions

- Quality assurance and data security administration
- Help desk and telecommunication networks
- Job control analysis and job scheduling
- Tape librarian and documentation librarian
- Systems analysis and application programming

(vi) Network Management

Topics covered in network management include architecture, management categories, changes, and interoperability.

(A) Network Architecture Network architecture is a plan describing the design of software, firmware, and hardware components that make up a data communication system. The functions performed by software or firmware are divided into independent **layers**. Each layer isolates the layers above it from the complexities below. The network architecture also defines protocols, rules, standards, and message formats to which different hardware and software vendors must conform in order to achieve given customer data communication needs and objectives. The major goals of network architecture are ease of use, reliability, connectivity, modularity, and ease of implementation and maintenance.

(B) Network Management Categories Network management deals with six categories.

1. **Network architecture** specifies network management functions that are essential building elements for a network management system from an architectural point of view.
2. **Configuration management** is concerned with initializing a network and gracefully shutting down part or all of the network.

3. **Fault management** encompasses fault detection, isolation, and the correction of abnormal operations.
4. **Security management** supports the application of security policies.
5. **Performance management** allows evaluation of the behavior of resources in the open system and of the effectiveness of communication activities.
6. **Accounting management** enables charges to be established for the use of resources in the open system and for costs to be identified for the use of those resources.

(C) Network Changes Network changes are many and common in any computer center. Unauthorized, incomplete, or incorrect network changes can have an adverse effect on a computer center's security, integrity, and operations. Adequate and timely procedures are needed to define clearly who should do what, when, and how. Some examples of network changes are listed next.

- Adding, changing, or deleting a user to access computer systems and data files (e.g., application systems, databases, e-mail, and utility programs)
- Adding, changing, or removing:
  - A terminal, printer, or a PC connection or its location
  - Network data lines and circuits
  - A modem (dial-in) connection to inter- and intra-organization computers
  - Other related network devices, connections (e.g., gateways, LANs, WANs, metropolitan area networks [MANs], and value-added networks [VANs]), and their definitions
- Adding a person to use the voicemail and voice-answering telephone system

A network change request can from many sources, either on paper or phone or via other media. Regardless of request media, basic information is required for effective and timely service, such as user name, user/terminal/controller ID, hardware device model/serial number and location, modem type (external/ internal), network port number, logical address of the hardware device, control unit address, request date, and date service needed.

If the current paper-based network change request mechanism is slow and ineffective, a computer-based approach should be considered. The change request can be entered electronically by the requestor, can be routed to various personnel who process the request, and can be updated by the person who completed it, and the status (e.g., closed, open, deferred, pending, and waiting) can be inquired by the requestor or other interested parties.

(D) Network Interoperability The computing environment of many organizations today consists of hardware, systems software, applications software, printers, protocols, and terminals acquired from different vendors with different platforms. Problems abound in terms of the ability of computers to talk to each other. Data cannot be extracted from these systems easily and quickly so management can get a consolidated view of the business operations and performance. Decisions are made without complete information, and available information is normally out of date.

The ideal goal for the network management in providing network interoperability is to:

1. Minimize the costs of handling data.
2. Minimize the learning curve in accessing new data.

3. Increase data integrity.
4. Increase system reliability.

The question is how to integrate data from a variety of dissimilar platforms, systems, and computers acquired from different vendors. Interoperability of systems is becoming a prerequisite to operate and manage in local and global markets and to handle competition. A major stumbling point in the struggle toward interoperability today is the lack of a global, distributed naming standards and directory services that would help users find services in geographically dispersed networks.

(e) Enterprise-Wide Resource Planning System, Customer Relationship Management System, and Software Licensing and Piracy Management

The section covers enterprise-wide resource planning (ERP) system, CRM systems, and software licensing and piracy management. Specifically, this section discusses the advantages and disadvantages of ERP systems, benefits from the CRM system, and piracy and legal risks from using illegal or unauthorized software.

(i) Enterprise-Wide Resource Planning System

(A) Overview of ERP System An ERP system is software that can help organizations in optimizing their value chain, which requires integrating business processes across organizational boundaries through IT.

Value chain = Business process reengineering + Change management + ERP

ERP systems allow employees to access a full database of information that will allow them to complete their tasks. The information can also be shared with customers and suppliers as needed. The ERP system can track business transactions from their origin (at the customer) to order entry through operations and accounting until the transaction is completed. The objective of ERP systems is to integrate all functions within an organization and to become customer-oriented (customer-centric). Companies are using ERP systems for increased business competitiveness.

The SAP R3 system is an example of ERP. Its objective is to standardize business processes across business units, functional departments, and product lines. R3 is the broadest and most feature-rich ERP system. SAP provides collaborative e-business solutions between companies and their customers and suppliers. More specifically, SAP integrates front-office and back-office systems, internal and external systems, and unstructured and structured information. The IT department will play a major role in implementing ERP systems.

SAP and other vendors use push technology to deliver critical software or information over the Internet to their customers. Push technology is an automatic transmission of information over the Internet rather than making users search for it with their browsers. Advantages of push technology are speed and convenience; disadvantages include information overload and clogging up the Internet communications links with data traffic.

(B) Advantages and Disadvantages of ERP Systems **Advantages** of ERP systems include: elimination of costly, inflexible legacy systems; improvement of work processes; increase in access to data for operational decision making; and standardization of IT infrastructure (hardware, software, OSs, and databases). **Disadvantages** of ERP systems include: expense and time in implementation, difficulty in implementing change in the organization, risks in using one vendor, and difficulty in integrating with other computer systems.

(ii) Customer Relationship Management System

Marketing departments are acquiring or developing a CRM system to survive in the customer-centric environment and to establish a one-to-one business relationship with customers. Some define CRM as a call center solution. Some view it as sales force automation; others as direct mail, marketing automation, or simply a Web page. Many companies see it as a "front-end" application only, interacting at the point of contact, point of purchase, or customer support. Others believe the secret to CRM success is in the "back-end" activities, such as data mining, data warehousing, data distribution, and data sharing. A properly designed and implemented CRM system encompasses all of these and much more. It is better to view the CRM system as a bridge system, not as a front-end system or back-end system.

To derive benefits from the CRM system, organizations **must:**

- Understand that customers come first, products and services come next.
- Understand the customer cycle as "get, keep, grow" or "acquire, support, retain."
- Understand that customers "pull" the company's products or services of their choice.
- Understand that marketers "push" company's products or services on to customers.
- Understand that pull and push concepts must be linked together to create interactive, learning relationships between the company and its customers. This linkage, in turn, results in increasing customer satisfaction and loyalty, share of customer, return on sales (ROS), and return on investment (ROI).
- Establish a strong linkage between the CRM system and financial performance such as ROS and ROI.

(iii) Software Licensing and Piracy Management

Similar to systems and network devices, OS software and application software are also relevant data sources or assets for organizations. Software asset and licensing information may be centrally managed by a software asset management tool to track license compliance, monitor usage status, and manage the software asset life cycle. Software license management tools offer a variety of features to automate inventory, utilization monitoring and restrictions, deployment, and patches for software.

A periodic **audit** of software licenses should be conducted to mitigate legal liabilities with software vendors. Ineffective and inefficient management of software license issues can lead to software piracy risks.

Software monitoring is performed to determine illegal acquisition of software and unauthorized use of software. Audit software running on a computer will detect illegal acquisition, which is using unofficially acquired software. This audit can be performed either manually or with automated tools. For example, an organization may audit systems for illegal copies of copyrighted software. This problem is primarily associated with PCs and LANs but can apply to any type of computer system or mobile devices. Another requirement is retention of business records to comply with legal, tax, audit, and regulatory authorities.

Many organizations use a **software metering program** to ensure that software is properly licensed, as required. System users are defined to the software metering product, and the product controls and monitors who is using the system and determines whether the user is authorized to use the system. Unauthorized users will be denied access to the system.

Risks from illegal software include:

1. Telecommuting employees may install on their home computer, which is also used for business purposes, illegal software that is not authorized by their employers.
2. Regular employees may bring software from home to work that is not authorized by their employers.
3. Disgruntled employees may report illegal copying and using of vendor-developed software to government officers, software vendor representatives, or software alliance or watchdog groups.

Developing and monitoring a software inventory management system is an effective control to detect illegal use of copyrighted software.

The purpose of the U.S. Executive Order on computer **software piracy** is to prevent and combat computer software piracy by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of U.S. federal law, including the Copyright Act.

(A) Software Licensing Practices Internal auditors need to be familiar with many variations of available software licensing practices.

The next list indicates how software is licensed for PCs, LANs, and workstations:

- Major characteristics of the application, whether it is a single-user or multiple-user application
- Major classification of software agreements, such as single-user program or multiple-user software
- Multiuser software is further subdivided into site licenses, per-server licenses, per-PC licenses, and number-of-users licenses.
- Maximum number of concurrent users. Regardless of the machine in use, a LAN software license can be bought only for the number of employees who would use the software simultaneously. Either a LAN OS or a utility program can monitor concurrent access to the software on a network.
- Floating licenses. In a client-server environment, often a single copy of a software program is bought and a client license is obtained for each workstation. In this arrangement, the specified number of licenses are bought and that only required workstations can use it. It does not matter who uses the workstations as long as the number of users does not exceed the number contracted for. Floating licenses are distributed by the server when a license request is received from a client.

Auditors should be aware of these requirements for a successful and complete software contract negotiation:

- The basis for the license per CPU machine
- Specifying most-favored-customer status generally through price concessions

- Arbitration clauses where disputes are submitted for binding arbitration
- Cancellation clauses with time periods and charges required
- Software fixes, upgrades, and future options
- Responsibility for the independent or subcontractors hired and provided by the vendor
- Responsibility for inherent defects in the software or hardware
- Insurance requirements on the software product or the hardware device
- Software and hardware maintenance requirements
- Notification of unauthorized use or possession of vendor software
- Document and software reproduction rights and limitations
- Computer virus damage, detection, and prevention requirements
- Access to source code and its modifications
- Global use of software and hardware

Auditors should be aware of these legal and contractual issues when end users directly acquire or use software from third parties or software publishers:

- The end-user licensing agreement is a legal contract between a buyer or acquirer (end user) and a seller (third parties or software publishers). It spells out the terms and conditions for using the software. The agreement might say that only the buyer can install the software on the buyer's computer for personal use, that the buyer agrees to third-party monitoring of the software, or that allow are gratned access to parts of the buyer's computer.
- The licensing agreement can affect the buyer's online security, privacy, flexibility, and freedom. Specifically, the buyer should be concerned about agreements that allow the software publisher or third parties to:
  - Monitor the buyer's Internet activity.
  - Collect the buyer's personal information.
  - Use or share the buyer's computing resources or information.
  - Hold the buyer accountable for the software agreements governing third-party software components.
- Most agreements limit the buyer's ability to sue the third party or the publisher for any damages cause by using the software.
- The use of "free" software or peer-to-peer (P2P) file-sharing software can be risky because it might require the buyer to exchange some personal information in order to use the free software.
- Cascading end-user licensing agreements can be very risky due to several unknown and intermediate firms involved in the production and distribution of the final software that the buyer is acquiring or using. There could be a primary software vendor, an upstream third-party software vendor, or a downstream third-party software vendor; each vendor may force the buyer to accept its own licensing agreements. It might be surprising to know whether the primary software vendor fully knows about the use of upstream or downstream vendors' software components that went into to the final software and the terms and conditions required of these third-party software licensing agreements.

(B) Software Piracy The vast majority of the software involved in software piracy legal cases is off-the-shelf, PC software, such as word processing, spreadsheets, graphics, and databases. The issue is illegal use, copying, and distribution of software both inside and outside the organization. Here "illegal" means that a user has not paid for the software.

Software piracy policies are needed to protect the organization from legal suits by owners. The policy should include:

- Prohibiting illegal copy and use of software.
- Developing a software inventory management system that includes a list of popular application programs. This list can be compared to the organization's purchase orders, original software diskettes, or original documentation manual.
- Periodically checking PC hard disks for illegally copied software.
- Making illegal copying of software grounds for employee dismissal.
- Requiring all employees to sign a statement that they will not use illegal software at work and not use the illegal software taken from home to work.
- Prohibiting copying of internally developed software.
- Prohibiting pirated externally developed software from being brought into the organization.
- Monitoring of all sensitive programs from illegal copying.

(C) Copyright Laws Copyright laws protect software. The act of illegally (not paying for) copying, duplicating, or using the software is called software piracy. Internet piracy involves illegally gaining access to and using the Internet. Many companies on the Internet receive customer fees for their research, services, information (e.g., sports and market analysis), and products. When unauthorized people use such services illegally, Internet firms lose revenues. Both software piracy and the Internet piracy are growing steadily.

Copyright laws give protection to the author for almost anything he or she created that can be expressed in a tangible form. Under the law, only the author or copyright owner may make copies unless permission is granted to others. When the author sells the copyright, the new owner takes over all the rights and privileges of the author.

Computer programs are copyrightable. Source code, microcode, and object code can be copyrighted. Blank forms can be copyrighted if they convey some information by their organization and have considerable originality. Similarly, computer terminal screens can be copyrighted if they are part of a computer program and vice versa. However, procedures, concepts, and principles cannot be copyrighted.

One computer program is said to be an **infringement** on another when the alleged infringing product and the copyrighted product contain many similar design features and functions. Although the structure, sequence, and organization of a computer program is protected by copyright, the physical order of the subroutines and their calling sequences are not protected.

Input formats are copyrightable in some courts but not in others. Statistical formulas are not copyrightable when they are used in an input format. Even innocent or unintentional infringers may be liable for using a copyrighted material without the written permission of the owner.

Legal penalties for copyright infringement may include injunction, punitive damages, and possible criminal prosecution. However, penalties do not include payment of actual damages as well as any profits. Attorneys' fees and costs may be awarded.

Fair use is a defense against a charge of copyright infringement. Fair use depends on the:

- Amount of material and economic impact of the material that was "taken."
- Nature of the copyrighted work.
- Nature and purpose of the use (i.e., whether it is commercial or not).

When a teacher copies substantial portions of a text for students, it is not a fair use. If what is copied is a small portion of the text, it would come under fair use. *Selling illegal copies of software for profit would not be fair use, whereas making one backup copy for archival purposes would be fair use.*

When consultants, software developers, and employees are doing work for an organization, the organization becomes the owner of the work products. In order for an organization to claim product ownership, the work should be a part of an employee's job description.

(D) Penalties in Contracts If the customer/client refuses to pay due to nonperformance by a vendor/contractor, can the contractor "electronically repossess" the software that he or she developed/maintained for or supplied to the customer? The question is: Who is right?

Even where it is clear that the client wrongfully refused to pay for the contractor's work, electronic repossession of software is not always justified. The contractor/developer's claim for payments due does not automatically include a right to repossess or disable the software, especially without going to the court. One exception is when the contractor is the owner or has a personal property interest in the software product. Disabling of computer software could interrupt business operations and customer services.

Even where the vendor has an arguable right to "repossess" or disable the software, the manner in which the repossession is executed may itself be wrongful. If a contractor/developer must access the customer/client's computer in order to remove or disable the software, this may constitute a violation of federal and/or state computer crime statutes.

If a contractor disables the client's software, the client can sue the contractor for trespass, intentional interference with contractual relations, and breach of contract.

Automatic disabling mechanisms, such as time/logic bombs, drop-dead devices, Trojan horses, and access keys, are illegal and unauthorized program code inserted into the computer system, to be activated by the system date on the computer, by turning up a counter, or by occurrence of some specific event or condition.

Software disabling mechanisms by vendor/contractor require advance notice to the client (i.e., clients must be notified prior to entering into a software agreement).

Courts do not appreciate the idea that business operations are at the mercy of, or slave to, a computer. The courts would prohibit the vendor from activating the drop-dead device if prior notice is not given to the customer. However, courts would allow a vendor to activate a

drop-dead device where notice of the device was included in the contract. In either case, such contractual protection will not protect the vendor/contractor if the vendor itself is in default (i.e., nonperformance).

(E) Acceptance Testing of Contracts The next list provides guidelines for acceptance testing of software contracts.

- A well-drafted contract will not guarantee the quality of software development and maintenance work, but it can provide the developer a strong incentive to do the job right, and it can give the client some legal protection in the event there is a problem.
- Every software acquisition or development contract should include one element: the right to conduct an acceptance test. Successful completion of an acceptance test should be a condition that must be met before final payment is made to the contractor or vendor. If the software does not perform properly, the final payment should be withheld until the contractor/vendor corrects the problem, refunds the amounts previously paid, fixes the software without pay, or provides some other remedy.
- Defining what constitutes acceptance testing is a major question and concern. Here the buyer or the client needs to evaluate both the performance and the reliability of the software. It is important that the specifications contained in the contract be clear, thorough, and complete since the test results are measured against these specifications.

The contract should define the obligations of each party during the acceptance test. The contract should specify, for example:

- Whether the test is done by the client, vendor, third party, or in combination.
- Who supplies or prepares the test data.
- Who corrects software problems during the test.
- How long postinstallation support is provided.
- What happens if the software fails, is defective or inoperable. The fallback plan must be specified.
- How the software acceptance is to be communicated.
- When the warranty begins.

When the software does not work as expected, the customer can:

- Return the software.
- Cancel the contract.
- Obtain a refund of all or partial sums paid.
- Accept the defective software at a reduced price.

(f) Data and Network Communications and Connections

This section is divided into two major parts for clarity and simplicity: (1) computer data and communications networks and (2) network connections.

(i) Computer Data and Communications Networks

Computer networks can be classified according to their scale and location similar to classifying multiple processors based on their physical size. Wired networks include personal area networks (PANs), LANs, MANs, WANs, and the Internet. Wireless networks include wireless PANs (WPANs), wireless LANs (WLANs), wireless MANs (WMANs), wireless WANs (WWANs), and wireless cellular networks. In addition, campus-area networks, broadband networks, Voice over Internet Protocol (VoIP), voice-mail network systems, private branch exchange (PBX) systems, plain old telephone services, VPNs, multimedia collaborative computing systems, ad hoc networks, content delivery networks (CDNs), VANs, wireless sensor networks, digital cellular networks, peer-to-peer networks, converged networks, optical networks, body area networks, and radio frequency identification networks are presented.

(A) Wired Networks The lowest scale of wired network is a **PAN** or home network in a room for an individual's use or to conduct home-based business. For example, a wireless network connecting a computer (e.g., desktop PC, laptop PC, notebook PC, tablet PC, and personal digital assistant [PDA]) with its mouse, keyboard, and printer is a PAN or home network.

The next highest scale of wired network is a **LAN** for use in a single building or campus of buildings connected by PCs and workstations to share peripheral resources (e.g., printers and scanners) and to exchange information. Several topologies are possible for broadcast LANs, such as bus, star, tree, ring, and mesh. The combination of a cable and host forms a LAN, and there is no subnet for LANs.

The next highest scale of wired network is a **MAN** for use in a city for cable television network. MANs are also called wireless local loops. It interfaces to the network layer and uses packet protocols (e.g., IP, PPP, and Ethernet), which are connectionless, and asynchronous transfer mode (ATM), which is connection oriented. It requires mapping the ATM connection to the other connections.

The next highest scale of wired network is **WAN** for use in a country or continent to run user application systems. A WAN consists of hosts (PCs) that are connected by a communication subnet. The subnet consists of transmission lines and switching elements (routers). Transmission lines move bits between computers using copper wire, optical fiber, or radio links. Routers connect three or more transmission lines. Customers own the hosts whereas telephone companies or ISPs own and operate the communication subnet. The combination of a subnet and its hosts forms a WAN.

The highest scale of wired network is the **Internet** for use on all continents (i.e., the entire planet). An internetwork (Internet) is established when distinct networks are interconnected (e.g., connecting a LAN and a WAN or connecting two LANs).

(B) Wireless Networks **WPANs** are short-range wireless networks (e.g., Bluetooth), using the IEEE 802.15 standard. They connect computer components without wires and using short-range radio and use open standards for short-range communications.

WLANs, using the IEEE 802.11 standard (Wi-Fi), communicate with other systems through a radio modem and antenna. They are used when installing the Ethernet is not feasible, as in office buildings, airports, hotels, restaurants, and campuses. WLANs serve as an extension to existing wired LANs.

The IEEE 802.11 standard defines how to design interoperable WLAN equipment that provides a variety of capabilities, including a wide range of data rates, quality of service, reliability, range optimization, device link options, network management, and security.

WLANs provide five distribution services (i.e., association, disassociation, reassociation, distribution, and integration) and four station services (i.e., authentication, deauthentication, privacy, and data delivery). Distribution services relate to managing cell activities and interacting with stations outside the cell. Station services relate to activity within a single cell (intracell), and occur only after the distribution services have taken place.

WMANs, which are fixed broadband networks, are used for high-speed wireless Internet access jobs in a city using IEEE802.16 standard known as Worldwide Interoperability for Microwave Access ((WiMAX). It is intended for wireless MAN and provides seamless mobile access in much the same as wide-area cellular networks with higher transmission speeds. Security advantages of WiMAX include mutual device/user authentication, improved traffic encryption, and options for securing data within the core network.

WWANs, using the IEEE 802.11 standard, are installed for cellular telephone systems using the radio network. A WLAN bridge can connect multiple LANS to form a WAN. Wireless supports varying distances with a direct line of sight. WWANs are similar to WLANs except that the distances involved are much greater and the bit rates are much slower. WWANs use low bandwidth.

Wireless cellular networks are managed by service providers that provide coverage based on dividing a large geographical service area into smaller areas of coverage called cells. As a mobile phone moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection.

Cellular networks support cellular phones, smart phones, and cellular data cards. Smart phones offer more functionality than basic cellular phones, including e-mail and Web browsing wirelessly (e.g., Bluetooth and Wi-Fi). Cellular data cards allow laptop users to connect to the Internet anywhere cellular service is available. However, cellular data cards can access the Internet only if the user is within the service provider's network coverage area.

WHAT ARE WIRELESS TECHNOLOGIES?

Wireless technologies include:

- Bluetooth technology is used in laptop computers, PDAs, and other mobile devices.
- Wireless closed circuit television (CCTV) technology is used in surveillance and monitoring.
- Radio frequency (RF) identification technology is used in identification and tracking of items.
- 802.11 technology is used in WLANs.
- Mobile radio technology is used in radio transmissions.
- Wireless mesh network technology is used in transporting data.
- Cellular technology is used in cellular modems, routers, and bridges for high-speed wireless data.
- WiMAX technology used in WMANs.
- Microwave and satellite technology is used in cell phones, PDAs, radio, cable, infrared, and air lasers.

(C) Wired Local Area Networks A wired LAN is a network that interconnects systems located in a small geographic area, such as an office, all the computers in one building, or all the computers in several buildings in close proximity (i.e., in a campus). LANs can be classified in a number of different ways. Four commonly used classifications include topology, transmission controls, transmission medium, and architectural design.

LAN Architecture Choosing a LAN software or hardware configuration that will support the desired functional and security features requires an understanding of LAN architectures. Two popular logical architectures that are supported on PC-LANs today include client/server architecture and peer-to-peer architecture.

LAN Concepts Various concepts in wired LANs are listed next.

- LAN basic topologies include star, bus, ring, tree, and mesh.
- LAN media access control methods include Ethernet (IEEE 802.3), token bus (IEEE 802.4), IBM token ring (IEEE 802.5), and Fiber Distributed Data Interface (FDDI).
- IP, which is a packet protocol, is a connectionless protocol so it fits well with the connectionless Ethernet protocol.
- The LAN transmission media include twisted-pair wire, coaxial cable, and fiber optic cable.
- LAN transmission methods include unicast, broadcast, and multicast.
- LAN internetworking devices include routers, bridges, brouters, repeaters, switches, hubs, and gateways.
- FDDI and fiber channel are two ring-based optical LANs, used as backbone networks, and are not successful at the desktop-level use.
- FDDI offers an optional bypass switch at each node for addressing failures.
- LANs can link to WANs and other networks using the Internet.
- LANs may use client/server or peer-to-peer architecture.
- Transmission media can be guided or unguided.
- Examples of guided transmission media include twisted-pair wire, coaxial cable, and fiber optic cable.
- Examples of unguided transmission media include radio, microwave, infrared, and air lasers.

LAN Security Goals and Features There are four LAN security goals.

1. Maintain the confidentiality of data as they are stored, processed, or transmitted on a LAN.
2. Maintain the integrity of data they are stored, processed, or transmitted on a LAN.
3. Maintain the availability of data stored on a LAN and the ability to process and transmit the data in a timely manner.
4. Ensure the identity of the sender and receiver of a message.

LAN Security Concerns and Risks Major security concerns and risks of LANs are listed next.

- Distributed file storing (file servers controlling user access to files)
- Remote computing (servers authenticating remote users, system components and applications)
- Topologies and protocols (messages reaching the desired destination)
- Messaging services (protecting e-mail during transit and in storage)

Other security concerns and risks are listed next.

- Possible inherent threats in LANs include both active and passive wiretapping.
- Passive wiretapping includes not only information release but also traffic analysis (using addresses, other header data, message length, and message frequency).
- Active wiretapping includes message stream modifications, including delay, duplication, modification, deletion, or counterfeiting.
- A single-link failure, a repeater failure, or a break in the cable could disable a large part or the entire network.
- When two or more stations transmit at the same time, data frames will collide, leading to unpredictable results and garbled transmission. Neither one gets through. "Who goes next?" is the problem to be resolved. The number of **collisions** will increase as the channel's load increases. When two frames collide, the medium remains unusable for the duration of transmission of both damaged frames. Collision detectors are needed to resolve collision.
- There may not be a backup person for the LAN administrator.
- The backup person, even though designated, may not have been trained adequately to take over the LAN administrator's job duties when needed.
- Changes made to the LAN network may not be transparent to end users.
- LANs can become single points of failure due to vulnerable cables and connectivity hardware.
- Inadequate LAN management and security policies.
- Lack of training of employees for proper LAN usage and security.
- Inadequate protection mechanisms in the workstation environment.
- Inadequate protection during transmission.

LAN High-Security and Low-Security Features A **high-security LAN** might include these features:

- Dedicated file server using client/server architecture
- Diskless PCs or workstations remotely booted
- Logical access security control down to the lowest level possible (i.e., byte level)
- Encryption of passwords
- Password format control
- Security monitoring, accounting, and reporting

- Network encryption devices
- No disk format command
- Image backup utility programs
- Fault-tolerance design with the use of disk-mirroring, disk-duplicating, or server-mirroring methods
- Reduced system privileges to directories, files, or records
- No remote log-in feature
- Automatic log-out feature after some dormant period
- Printers attached to secured file server

A **low-security LAN** might include these features:

- Peer-to-peer architecture
- Allows disk format command
- Shareable printers across the network
- Bootable workstations with local storage facilities
- No directory-, file-, record-, byte-level access controls
- Basic, simple password protection

Client/Server Architecture Many definitions exist for client/server systems. One broad definition is the coordination of data as application systems are distributed. The application system's processing is divided into two parts: (1) client, where users request data services, and (2) server, which furnishes the requested data to the user client. In other words, Web pages, documents, and files (e.g., data, video, and audio) are transferred from the server to the client.

Client/server architecture is similar to cooperative processing, which enables the application system to be divided across multiple, different hardware platforms. In other words, the computing process is distributed across multiple, different hardware platforms. This contrasts with distributed processing in that the entire computing process is distributed among several similar platforms. In cooperative processing, a single computing process uses several different connected platforms. With distributed processing, a single computing process runs independently on multiple, similar platforms.

Typical hardware components required in a client/server environment include a PC or workstation capable of storing data, a terminal emulation device, and a physical connection to the host computer system. Servers are powerful computers providing the client computers with a variety of data services. The client and the server are linked via a LAN or other data communications system. The flow of data is mostly one way (i.e., from the server to the client).

There are six basic elements of the client/server computing process:

1. Data storage
2. Database management system
3. Application system

4. Operating system (OS)
5. Display device
6. User interface

Elements 1 and 2 are located on the server or host platform, and elements 3 through 6 are located on the client platform.

The normal client/server implementation is a two-tiered architecture for simple networks (i.e., one client and one server) and multi-tiered (*n*-tier) is possible for complex networks. In *n*-tier architecture, there is one client and several servers (e.g., Web server, application server, database server, and others) where client requests are handled by different levels of servers.

Most client/server systems are designed for PCs and LAN-based OSs. The processing of an application is split between a front-end portion executing on a PC or workstation (client) and a back-end portion running on a server. Exhibit 6.14 provides an overview of the client/server functions.

Client functions	Server functions
Contains front-end programs	Contains back-end programs
Provides data entry and data manipulation	Facilitates access to the data
Handles ad hoc queries	Accepts and process the data
Invoked by a user	Invoked by a client
Provides management reporting	Provides locking and logging mechanisms
Runs batch jobs	Places data in the database
Users cannot access the data in the server directly	Returns the data and status codes to the client upon request
Needs heavy user interface	Needs no user interface
Provides user-friendly interaction	Provides system backups, database synchronization, and database protection
Uses diskless PCs or workstations for better security	Uses strong security controls to protect servers (e.g., SSL/TLS for authentication and encryption; mirrored or shadowed disks; shared buffering; fault tolerance mechanisms, such as automatic fail-over)

EXHIBIT 6.14 Overview of Client/Server Functions

Four client/server implementation approaches include:

1. Simple file transfer.
2. Application programming interface (API).
3. Graphical user interface (GUI)–based OS.
4. Peer-to-peer (P2P) communications.

The **simple file transfer approach** involves the transfer of data from a host server to a client workstation, PC, or LAN. The client application then accesses and processes the data. In addition

to the physical connection, the workstation requires emulation software to allow it to function as a host terminal. This approach is least costly and least complex to implement; costs little to integrate data; and is good for situations where access to real-time data is not required. With this approach, information associated with each physical database access must flow across the network. This approach assumes that the database resides on one processor and that the application program that accesses the database resides on some other processor.

The **API approach** links the client application with existing host applications. It requires no modifications to existing applications and requires no specialized programming skills. This approach is a first step in implementing more client/server strategies. The API provides a GUI with an existing character-based mainframe application system.

The **GUI-based OS approach** conforms to the true client/server model and is used in combination with an SQL database. Development costs may be high if there is a lack of in-house IT expertise and retraining is required. This approach is suited for situations where there is a need for access to updated information, and multiple client applications access the database. With this approach, only the initial query and the final result need to flow across the network. This approach assumes that the database resides on one processor and that the application program that accesses the database resides on some other processor. A GUI-based application and user-centered applications would reduce the amount of end-user training required on applications software.

The **P2P communications approach** does not use a hierarchical configuration, unlike the other three approaches. It allows applications to interact with each other on an equal basis. Any platform may act as a client, a server, or both. This approach is expensive, uses more system resources, requires greater programming skills, and is highly complex. Extensive rewrites of existing software are needed. This approach is well suited for situations where there is an availability of host data and there is a need to access or integrate data on multiple platforms and for a common interface.

P2P architecture requires no dedicated file server because any node on the network may selectively share its local hard disk with other nodes on the network. Other peripherals, such as printers, may also be shared across the LAN. This is a good choice for smaller LAN installations as it has a lower cost-per-node rate. However, significant security problems exist because of the lack of centralized data storage across the network. Typically, the architecture also has lower performance and requires greater administrative effort to configure and maintain security definition.

(D) Virtual Local Area Networks VLAN technology is an efficient way of grouping users into workgroups to share the same network address space regardless of their physical location on the network. VLAN separates the logical topology of the LANs from their physical topology and employs the IEEE 802.1Q standard. Users can be organized into separate VLANs according to their department, location, function, application, physical address, logical address, or protocol. Regardless of the organization method used, the goal with any VLAN is to group users into separate communities that share the same resource, thereby enabling the majority of their traffic to stay within the boundaries of the VLAN.

The logical separation of users and traffic result in a better performance management (i.e., broadcast and bandwidth utilization control). It also facilitates a reduction in configuration management overhead, enabling networks to scale at ease. By default, all ports are configured to be members of VLAN1, which is all untagged traffic. As a consequence, VLAN1 may unwisely span the entire

network if not appropriately controlled. The risk is even greater if VLAN1 is also used for user VLANs or the management of VLAN. In addition, it is unwise to mix management traffic with user traffic, which makes the management of VLAN an easier target for exploitation.

Trunk links can carry the traffic of multiple VLANs simultaneously. Therein lies a potential security exposure. Trunk links have a native or default VLAN that is used to negotiate trunk status and exchange VLAN configuration information. Trunking also enables a single port to become part of multiple VLANs—another potential security exposure.

The system administrator for VLAN will ensure that:

- VLAN1 is not used for in-band management traffic. It is good to use a dedicated management VLAN to keep management traffic separate from user data and control plane traffic.
- Management of VLAN is not configured on any trunk or access port that does not require it.
- VLAN1 is not used for user VLANs.
- VLAN1 is pruned from all trunk and access ports that do not require it.
- Trunking is disabled on all access ports.
- When trunking is necessary, a dedicated VLAN is configured for all trunk ports.
- Access ports are not assigned to the dedicated trunk VLAN.

Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Unauthorized internal access leads to the possibility of hackers or disgruntled employees gaining control of network resources, eavesdropping, or causing DoS on the network. Simply connecting a workstation or laptop to a wall plate or access point located in the work area enables internal access to the private network.

The **port security** feature provided by most switch vendors can be used to block input to the access port when the media access control (MAC) address of the station attempting to access the port does not match any of the MAC addresses specified for that port (i.e., those addresses statically configured or auto-configured [i.e., learned]). The maximum number of MAC addresses that can be configured or learned (or combination of both) is also configurable.

The system administrator for VLAN will ensure that:

- Disabled ports are placed in an unused VLAN.
- Port security or port authentication is used on all access ports.
- Port security has been implemented; the MAC addresses are statically configured on all access ports.
- If port authentication is implemented, reauthentication occurs every 60 minutes.
- If port authentication is implemented, all access ports must start in the unauthorized state.

(E) Wireless Local Area Networks The most widely implemented legacy WLAN technologies are based on the IEEE 802.11standard and its amendments, which are not capable of using the new

IEEE 802.11i standard that is used in robust security networks (RSNs). WLAN transmission protocols include Carrier Sense Multiple Access (CSMA), with Collision Avoidance (CSMA/CA), and with Collision Detection (CSMA/CD).

Legacy WLANs WLANs are groups of wireless networking nodes within a limited geographic area (e.g., an office building or building campus) that are capable of radio communication. WLANs are usually implemented as extensions to existing wired LANs to provide enhanced user mobility and network access. Legacy WLANs have limited and weak security controls and are particularly susceptible to loss of confidentiality, integrity, and availability. Unauthorized users have access to well-documented security flaws and exploits that can easily compromise an organization's systems and information, corrupt the organization's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use the organization's resources to launch attacks on other networks.

WHAT ARE THE POTENTIAL RISKS IN WLAN TECHNOLOGY?

Despite the availability of strong encryption for user communication, the management frames of IEEE 802.11 messages are not encrypted, leaving the door open for DoS attacks. Several tools (e.g., Wi-Fi jammers and rogue access points) are available that can cause users to drop off the network or send messages to hamper the functionality of wireless endpoints. Wi-Fi jammers are designed to block IEEE 802.11 transmissions. Rogue access points are set up in hopes of attracting connections, then stealing sensitive information or altering communications.

Note that Wi-Fi access points are often set up quickly and without security foresight. This results in the use of weak or no encryption, allowing attackers to impersonate wireless endpoints in hopes of providing false data. It also may result in users not changing default passwords for device management, allowing attackers to gain full control of the access point. There is also a possibility of worms and other malicious code propagating on the local network.

Robust Security Networks for WLANs Based on the IEEE 802.11i standard, robust security networks (RSNs) were found to remedy the security problems of wired equivalent piracy (WEP) as RSNs provide moderate to high levels of assurance against WLAN security threats through use of a variety of cryptographic techniques. The three types of RSN components are stations (STAs), access points (APs), and authentication servers (ASs).

(F) Campus-Area Networks A campus-area network (CAN) consists of LANs interconnected within multiple buildings or a short geographic area (e.g., a school campus, office towers, or military base). It can be safely assumed that all the threats, vulnerabilities, and risks applicable to LANs are equally applicable to CANs due to a common architecture.

(G) Wired Metropolitan Area Networks A wired MAN is configured for a larger geographical area than a LAN, ranging from several blocks of buildings to entire city, for cable television network. MANs can be owned and operated either as public utilities or as individual organizations. MANs interconnect two or more LANs. Although MANs depend on moderate-to-high data rates as required for LANs, the error rates and delays would be higher than might be obtained on a LAN. MAN is based on the IEEE 802.6 standard—distributed-queue dual-bus (DQDB) standard. Physically, a MAN consists of a transmission medium and nodes that provide user access to the medium. The DQDB standard is divided into three layers: upper, middle, and lower.

(H) Wireless Metropolitan-Area Network A WMAN employs the WiMAX communication technology using the IEEE 802.16 standard. WiMAX network threats focus on compromising the radio links between WiMAX nodes. These radio links support both line-of-sight (LOS) and non-line-of-sight (NLOS) signal propagation. Links from LOS WiMAX systems are generally harder to attack than those from NLOS systems because an adversary (attacker) would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. WiMAX NLOS systems provide wireless coverage over large geographic regions (e.g., the size of a city), which expands the potential staging area for both clients and adversaries. Like other wireless networking technologies, all WiMAX systems are susceptible to DoS attacks, eavesdropping, man-in-the-middle (MitM) attacks, message modification, and resource misappropriations.

(I) Wired Wide-Area Networks A wired WAN is a network that interconnects systems located in a large geographic area, such as a city, a continent, or several continents. A complex network can consist of WANs that span continents or geographic regions within continents and connect smaller, more localized LANs.

WANs connect intelligent terminals, workstations, PCs, minicomputers, and LANs together. They use public as well as private telecommunication facilities to accomplish this connection. For example, a WAN data link interconnection can be used to connect two or more physical LANs in different geographical locations. Some popular WAN protocols include Synchronous Data Link Control (SDLC), High-Level Data Link Control (HDLC), Link Access Procedure, Balanced (LAPB), and High-Speed Serial Interface (HSSI). The sequence of SDLC evolution is as follows:

$$\text{SDLC} \rightarrow \text{HDLC} \rightarrow \text{LAPB}$$

Types of WAN networks include switching networks. Switching is used to share communication channels between many users and can take place in the telephone exchange office, where the user dials into it using a telephone. The exchange can even take place on the user's premises, which enables many users to share a small number of access lines.

The four popular types of switching are message switching, circuit switching, packet switching and hybrid switching. With **message switching,** users can be interconnected on demand without using circuit switches. Messages are forwarded to a final destination (e.g., e-mail systems). In **circuit switching**, all the lines are connected to telephone exchange or switching offices. Individual users can lease telephone channels and install their own switches. **Packet switching** is another form of message switching used to interconnect all types of users on a general-purpose public data network. In this type, messages are broken up into smaller packets, which are routed independently through the network. The X.25 protocol standard is used in a packet switching network. **Hybrid switching** combines circuit switching and packet switching. Computer networks are usually packet switched, occasionally circuit switched, but seldom message switched due to transmission delays and throughput problems.

Fast packet networks, using fiber optic transmission, provide the necessary processing power to keep up with increases in link bandwidth and the necessary flexibility to support different kinds of services and a range of bandwidth requirements. Fast packet networks overcome the main weakness of traditional packet networks by using special control mechanisms to provide the consistent network performance required for video and other real-time services. In traditional

packet networks, such as the current Internet, the network may become heavily loaded in a way that degrades these services.

WHAT ARE THE MAJOR CONCEPTS IN A WIRED WIDE AREA NETWORK?

Some examples of major concepts in a wired WAN are listed next.

- WANs are packet-switched networks, meaning they use routers.
- WAN interconnection devices include bridges, repeaters, routers, switches, multiplexers, modems, and protocol converters.
- WAN networks include: private circuit networks (e.g., Integrated Services Digital Network [ISDN], XDSL, and public and leased lines), circuit-switched networks used in telephone company networks, and packet- switched networks (e.g., X.25, Frame Relay, link access procedure B (LAPB), Switched Multimegabit Data Services [SMDS], asynchronous transfer mode (ATM), packet transfer mode (PTM), and VoIP).
- WANs can become a single point of failure due to connecting several ISPs, networks, protocols, and communication lines and because of problems with their incompatibility and vulnerability.

The differences between a private (leased) line and public line are listed next.

- A private line provides voice and data transmission services without the public exchange.
- A public line provides voice and data transmission services with public exchange.
- If a private line fails, its users are cut off from the connection.
- If a public line fails, its users are provided with fallback procedures to recover from a disaster or malfunction.

The **X.25 standard** is an international standard that defines the interface between a computing device and a packet-switched data network WAN. X.25 implements point-to-point (PTP) connections between two or more user computers. It is a single point of connection for one user computer and a logical PTP connection for a number of user computers. This is accomplished through a concept called **virtual circuits** operating in either a permanent mode or a switched mode. The virtual circuits function in the network layer of the ISO/OSI Reference Model. By using X.25, one pays only for the bits sent, unlike circuit-switched or leased lines, where one pays for the time regardless of how much was sent. X.25 uses a high-speed shared connection, which is a predecessor to Frame Relay. Charging is typically by the packet, segment, or character and requires a connection before exchanging data, similar to a telephone call.

Advantages of X.25 virtual circuits include flexibility in providing a range of functions for implementing multiple-protocol enterprise internetworks when compared with the conventional telecommunication data links. **Disadvantages** of X.25 include additional overhead due to handling of multiple protocols and lower throughput due to complex routing decisions.

(J) Broadband Networks The capacity of a network, measured as the number of bits it can transmit every second, is called **bandwidth**. Broadband networks are high-bandwidth networks due in part to the use of optical fiber and high-speed switches. They carry video, sound, data, and image services. Broadband networks also allow a closer coupling of the computers on a network. Today, any kind of network transmitting at more than 100 million bits per second is considered a broadband network.

WHAT IS THE DIFFERENCE BETWEEN NARROWBAND NETWORKS AND BROADBAND NETWORKS?

- Narrowband network services include switching networks (WANs) and X.25 standard.
- Broadband networks include Frame Relay, Switched Multimegabit Data Services SMDS, ATM, PTM, ISDN, Digital Subscriber Line (DSL/ADSL), T lines and carriers, and cable Internet connections.
- Narrowband networks are low-bandwidth networks.
- Broadband networks are high-bandwidth networks.
- The dividing line between the two networks is not always clear and changes as technology evolves.

(K) Voice over Internet Protocol

VoIP Risks and Opportunities VoIP, is the transmission of voice over packet-switched IP networks. VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Because VoIP adds a number of complications to existing network technology, problems are magnified by security considerations.

Current VoIP systems use either a proprietary protocol or one of two standards: the H.323 gateway standard and the Session Initiation Protocol (SIP). An extension of SIP, the SIP for IM and presence leverage extensions (SIMPLE) standard, is being incorporated into products that support IM. In addition to H.323 and SIP, there are two other standards, Media Gateway Control Protocol (MGCP) and Megaco/H.248, which may be used in large deployments for gateway decomposition. Until a truly dominant standard emerges, organizations moving to VoIP should consider gateways and other network elements that support both H.323 and SIP.

The Internet Protocol security IPsec protocol was designed to provide interoperable, cryptographically based security for IPv4 and IPv6. The set of security services includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols. Thus, IPsec can be used to protect both VoIP signaling (i.e., SIP and H.323) and VoIP user traffic (i.e., Real-time Transport Protocol, [RTP]).

VoIP Control Guidelines VoIP can provide more flexible service at lower cost, but there are significant trade-offs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied into the data network, resulting in additional security weaknesses and avenues of attack.

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP compared with established telephony systems.

VoIP systems are unstable due to their reliance on packet networks as a transport medium. The public switched telephone network (PSTN) is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

VoIP General Controls An overview of general controls over VoIP is presented next.

- Separate voice and data on logically different networks. Different subnets with separate address blocks should be used for voice and data traffic, with separate DHCP servers for each.
- At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, MGCP, or Megaco/H.248 connections from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network management components. Strong authentication of clients toward a gateway is often very difficult. Here access control mechanisms and policy enforcement may help.
- Use firewalls designed for VoIP traffic, through either application-level gateways (ALGs) or firewall control proxies. Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call.
- Use IPsec or SSH protocol for all remote management and auditing access. If practical, avoid using remote management at all and do IP-based PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures that all VoIP traffic emanating from the enterprise network has been encrypted.

VoIP Physical Controls Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network-monitoring tools and tap into telephone conversations. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to monitor network traffic. Organizations therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, such as barriers, locks, access control systems, and security guards, are the first line of defense. Organizations must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks, such as insertion of sniffers or other network-monitoring devices. For example, installation of a sniffer could result in not just data but all voice communications being intercepted.

(L) Voice-mail Systems Voice-mail or voice messaging systems are computer-based systems with their own input, editing, storage, retrieval, and transmission of information in the form of natural (human) or synthetic speech. Voice-mail systems can be PC based or PBX based. Each user is given a voice mailbox for his or her own use. Outgoing and incoming messages can be of any length, or they can be fixed. All messages are date- and time-stamped.

Voice-mail systems interface with PBX systems, voice-response systems to place purchase orders or inquire status of an account balance in a financial/retail institution, and e-mail systems to remind that a voice-mail message is waiting while the user is on the e-mail session. See Exhibit 6.15 for risks and suggested controls for voice-mail systems.

There are two **advantages** for attackers to attack the phone system. The first advantage is that phone system attacks are hard to trace. It is possible to make connections through multiple switching units or to use unlisted or unused phone numbers to confound a tracing effort. Also, by being in the phone system, it is sometimes possible to monitor the phone company to see if a trace is initiated.

Potential or actual risks and exposures	Suggested controls
Toll fraud through voice-mail	Ensure that PINs are truly random; periodically change all PINs; use a lockout feature on failed attempts; remove all unassigned or unused mailboxes; unpublish the remote access number; block access to long-distance trunks and local lines; deactivate any mailboxes used by intruders; use voice encryption; restrict collect calls; and review telephone bills

EXHIBIT 6.15 Risks and Controls for Voice-Mail Systems

The second advantage is that a sophisticated host machine is not needed to originate an attack. Also, there is no need to have a direct access to the network to which the target system is attached. A simple unintelligent terminal connected to a modem can be used to initiate an attack. Often an attack consists of several hops, a procedure whereby one system is broken into and from that system another system is broken into, and so on. This again makes tracing more difficult.

(M) Private Branch Exchange Systems A PBX system is a sophisticated computer-based switch that can be thought of as a small in-house phone company. Failure to secure a PBX can result in exposing the organization to these issues:

- Toll fraud (most common)
- Disclosure of proprietary or confidential information due to eavesdropping
- Unauthorized access to routing and address data
- Data modification (changing billing information)
- DoS by making the equipment inoperable or forced to operate in a degraded state
- Traffic analysis (observing information about telephone calls and making inferences)
- Lack of external access controls over remote maintenance ports and access to the switch by a potentially large pool of outside parties
- Loss of revenue or legal entanglements

The threats to PBX telephone systems are many, depending on the goals of attackers. Exhibit 6.16 presents PBX risks and suggested controls.

(N) Plain Old Telephone Service Plain old telephone service (POTS) is a basic and conventional voice telephone system with a wireline (wired) telecommunication connection. It contains a POTS coder decoder (CODEC) as a digital audio device and a POTS filter (DSL filter). Three major components of POTS include local loops (analog twisted pairs going into houses and businesses), trunks (digital fiber optics connecting the switching offices), and switching offices (where calls are moved from one trunk to another). A potential risk or disadvantage of POTS is eavesdropping due to physical access to tap a telephone line or penetration of a switch. An advantage of POTS or mobile phone is that they can serve as a backup for PBX and VoIP system during a cable modem outage or DSL line outage.

(0) Virtual Private Networks A VPN is a virtual network, built on top of existing physical networks, provides a secure communications tunnel for data/information transmitted between networks. A

Potential or actual risks and exposures	Suggested controls
Toll fraud and other attacks through PBX	Reduce the time a modem is turned on; implement a two-factor authentication mechanism; use a lockout feature on failed attempts; install call detail recording and call accounting systems; use dial-up access to the PBX; use login control; log out when not in use; input command screening; use switch security features; control remote maintenance access; unpublish the remote access number; block all unassigned access codes; use multiple layers of security; install strong password management; protect modem pools; change system administrator passwords; block remote calling after business hours; restrict call transfer capabilities; protect telephone books; monitor PBX options and settings; and review telephone bills

EXHIBIT 6.16 PBX Risks and Controls

VPN is a protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated (leased) line. Because a VPN can be used over existing networks, such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. VPNs are usually established and managed by VPN gateway devices owned and managed by the organization being protected. Although VPNs can be implemented on top of ATM or Frame Relay, or over WAN connections, an increasingly popular approach is to build VPNs directly over the Internet. The leased lines (e.g., T1 and T3) are secure but expensive, and the Internet is less expensive.

The main components that make VPN secure are encrypted traffic and a protected authentication mechanism. The authentication method used can be a security token, known key, securely distributed certificate, password, or combination of any of these methods. Once the authentication is complete, the VPN should encrypt all traffic between endpoints to ensure no data are leaked and to prevent MitM attacks. Multifactor identification and authentication is strongly advised to neutralize the effectiveness of brute-force attacks. A common multifactor identification is a combination of a security token, known key, certificate, password, PIN, or biometrics.

A VPN can allow employees to connect to the intranet securely, so there are no fears of sensitive information leaving the network unprotected. The Internet alone cannot remove this fear.

A VPN is a private network composed of computers owned by a single organization that share information with each other in that organization (e.g., LAN or WAN). A public network is a large collection of organizations or computers that exchange information with each other (e.g., a public telephone system and the Internet).

A VPN blurs the line between a private and public network. With a VPN, a secure, private network can be created over a public network such as the Internet. A VPN can be created using software, hardware, or a combination of the two that provides a secure link between peers over a public network. Control techniques, such as encryption, packet tunneling, and firewalls, are used in a VPN. Tunneling encapsulates a packet within a packet to accommodate incompatible protocols. The packet within the packet could be of the same protocol or of a completely different one.

The private network is called virtual because it uses temporary connections that have no real physical presence but consist of packets routed over various computers on the Internet on an

ad hoc basis. Secure virtual connections are created between two computers, a computer and a network, or two networks. A VPN does not exist physically.

A VPN is a distributed collection of networks or systems that are interconnected via a public and/or private network but protects their communications using encryption. In effect, a VPN is a private secure distributed network that is transported or tunneled across a public and/or private network. Typically, VPN encryption is implemented at the local network entry points (i.e., the firewall or premise router), thereby freeing the end systems from having to provide the necessary encryption or communication security functions.

The VPN is configured to maintain the security of the enclave and the requirement that all traffic must pass through the enclave security architecture. This is not to say that encrypted data (e.g., SSL, SSH, and TSL) that entered the VPN tunnel must also be unencrypted prior to leaving the tunnel. However, the data would still have to pass through the respective application proxy. If host-to-host VPN is required, it will be established between trusted known hosts.

A VPN solution can be cheaper than conventional networks that run over WAN connections. VPN devices and software provide not only encryption functions but also network access control to secure Internet tunnels between remote sites. A VPN must provide privacy and integrity of data as they traverse the public network. At a minimum, it should provide user authentication, address management, and data encryption security services.

Four types of VPNs exist: SSL VPNs, IPsec VPNs, Encapsulating Security Payload (ESP) in tunnel mode, and firewall-based VPNs. Three primary models for IPsec VPN architectures include gateway to gateway, host to gateway, and host to host. Alternatives to IPsec VPNs include the ESP tunnel mode and firewall-based VPNs.

(P) Multimedia Collaborative Computing Networks Multimedia collaborative computing networks include IM architecture, Internet Relay Chat (IRC) architecture, remote (virtual) meeting technology, networked whiteboards, cameras, and microphones. Explicit indication of use includes signals to users when collaborative computing devices are activated.

The IM architectures vary in design depending on the services being provided to end users. There are four possible architectural designs for IM systems:

1. Private hosting (i.e., client to server)
2. Public hosting
3. Client to client
4. Public switched network

The four architectures differ in the location of the session data.

The IRC architecture consists of servers and clients. Servers form the backbone of the network, linking components together and using routing capabilities to relay messages to their destinations. All packets are relayed through the server, hence the name of the protocol. Clients reside on the machines of users who are chatting on the network. Currently, the IRC is mainly designed for group (many-to-many) communication in discussion forums called channels, but it also allows one-to-one communications via private message. IRC networks that are in operation need to migrate to newer IM technologies due to the inherent security vulnerabilities with IRC.

(Q) Ad Hoc Networks Networks of nodes that are near each other are called ad hoc networks, where both the routers and the hosts are mobile and running on the same computer (i.e., Nodes = Routers + Hosts). In traditional wired networks, the routers are fixed and the hosts are mobile. In ad hoc networks, topologies are changing all the time without warning. An ad hoc network is used when a group of users with notebook computers are gathered in an area where the IEEE 802.11 standard is not available. A common routing algorithm used in ad hoc networks is Ad hoc On-Demand Distance Vector, where it determines a route to some destination only when somebody wants to send a packet to that destination (i.e., as needed, meaning ad hoc). Bluetooth is a very popular ad hoc network standard.

(R) Content Delivery Networks (CDNs) CDNs are used to deliver the contents of music, movie, sports, or news from content owners' Web sites to end users quickly with the use of tools and techniques such as client caching, server replication, client's request redirection, and a proxy content server to enhance the Web performance in terms of optimizing the disk size and preload time.

Three parties exist in the CDN process to deliver the content to the end users: CDN provider (contractor), ISP, and the content owner (music or news provider).The CDN contractor delivers the content owner's material to the end users via the ISP for a fee. Server replication is called server mirroring, where the content is replicated at multiple, dispersed locations for end users' easy and quick access. The content is redirected without changing the DNS. Similar to caching, which improves the client's performance, mirroring improves the server's performance.

(S) Value-Added Networks Value-added carriers lease channels from other common carriers and then provide additional services to customers, using these leased channels. They operate a public data network, where the equipment breaks up the user's data into packets, routes the packets over its network between one location and another, and reassembles them into their original form on the other end. VANs take advantage of the economies of scale. Usually they share a wider bandwidth, which gives faster response time. Some examples of services provided by VANs include bulletin board services, Internet, electronic data interchange (EDI), and dial-in services, where the last two topics are covered next.

Electronic Data Interchange EDI uses proprietary communication structures and is the exchange of routine business transactions in a computer-processable format, covering such traditional applications as inquiries, planning, purchasing, acknowledgments, pricing, order status, scheduling, shipping and receiving, invoices, and payments. New ways of implementing EDI include the use of standardized communication structures such as eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Web services; and moving away from proprietary communication structures (e.g., VANs) to allow more interoperability and to facilitate better maintenance work.

Dial-In Services Many external, commercial electronic databases and online systems exist to satisfy a specific customer's need. Some systems provide general services, such as e-mail, real-time conferences, file transfer, game playing, and online news. Online search systems contain indexes from major magazines and other periodicals on all topics.

(T) Wireless Sensor Networks Wireless sensor networks (WSNs) are networks of interconnected wireless devices that are embedded into the physical environment to provide measurements of, for example, of a building security. These devices have built-in processing, storage, and RF sensors and antennas. These sensors start with a low-level sensors and progress toward nodes

for high-level data aggregation, analysis, and storage, where data are routed over a network to an automated computer facility. Typical applications of WSNs are listed next.

- Monitoring traffic or military activity
- Protecting physical property
- Monitoring environmental changes in a building (e.g., humidity, voltage, and temperature)
- Managing machinery and vehicle operation
- Establishing physical security perimeters for building and facilities
- Monitoring supply chain management activities
- Detecting the presence of chemical, biological, or radiological substances

(U) Digital Cellular Networks Today, separate networks are used for voice traffic (telephone traffic), computer communications (data networks such as the Internet), and video (broadcast or cable television or other specialized networks), which are expensive, time consuming, and complicated. A single digital network is needed that can potentially be used to transmit all types of data and information (i.e., voice, data, video, and images).

Digital cellular network standards in the world are varied and incompatible with each other. For example, the United States uses a CDMA standard whereas the rest of the world uses a Global System for Mobile Communications (GSM) standard. Today's cellular network systems are used to transmit both voice and data (e.g., a Short Message Service (SMS) to send and receive text messages). More powerful cellular networks use third-generation (3G) or fourth-generation (4G) networks to send and receive voice, data, video, and images.

(V) Peer-to-Peer Networks Broadly defined, peer-to-peer (P2P) network is a distributed computing software architecture that enables individual computers to connect to and communicate directly with other computers. Through this connection, computer users (known as peers) can share communications, processing power, and data files. With respect to file sharing specifically, P2P technology allows decentralized sharing. That is, rather than storing files in a central location to which individual computers must connect to retrieve the files, P2P technology enables individual computers to share directly among themselves files stored on the individual computers. P2P file-sharing programs themselves do not perform the sharing or copying of files; rather, they employ a protocol that facilitates communication between the two peers who wish to share or copy a particular file. Peers can share myriad types of files, including audio, video, software, word processing, and photographs.

By eliminating the need for a central storage point for files, P2P file-sharing technology allows for faster file transfers and conservation of bandwidth (i.e., the capacity to transmit information to and from a computer). In addition, because P2P technology decreases the need for businesses and consumers to store files on their hard drives, it can lower costs by conserving on storage requirements and saving on maintenance and energy costs related to data retrieval, sharing, and processing.

Uses of and risks from P2P technology include the following:

- P2P technology enables users to share communications, processing power, and data files with other users. Use of P2P technology can enhance efficiency by allowing faster file transfers, conserving bandwidth, and reducing or eliminating the need for central storage of files.

- P2P technology has a variety of applications, the most common application by far is commercial file-sharing software programs used by consumers to exchange files, such as music, movies, television programs, video games, software, and pornography.
- P2P technology continues to evolve in response to market and legal forces. It appears likely that the uses of P2P technology will expand in the future.
- Consumers face risks when using commercial P2P file-sharing software programs, including risks related to data security, spyware and adware, viruses, copyright infringement, and unwanted pornography.

(W) Converged Networks A converged network occurs when two different networks are combined, as in the case of data and voice networks. A converged network is subject to vulnerabilities and threats. For example, the same openings that allow voice traffic to pass unimpeded may also either create high-bandwidth covert channels for data infiltration or exfiltration or provide a point of entry for other probes and attacks. Although it may be impossible to examine voice traffic in real time without incurring unacceptable delay, it may be possible to isolate the voice traffic in some way from the rest of the network to minimize the vulnerabilities introduced by opening these entry points.

Although firewalls, hardware/software guards, and downgraders serve to separate an enclave from the outside world or the rest of the network, they may not limit latency, jitter, and delay problems in the context of the converged network.

A converged network is a *single point of failure* in a way that totally separate data and voice infrastructures were not because the converged network may not have uninterruptible power supply (UPS) and fault tolerance mechanisms to facilitate graceful degradation.

Until the technology improves, it might be preferable to isolate the packet-switched digital voice on a separate network from the data network. This isolation is a better approach rather than an ad-hoc box-based mix-and-match solution focused on individual functions.

(X) Optical Networks Optical networks use fiber-optic cables, which are strands of clear glass fiber. These cables are faster, lighter, secure, durable, expensive, and difficult to install. The optical network can transmit voice, data, and video with greater bandwidth. Existing optical networks can increase their capacity with dense wavelength division multiplexing (DWDM), which enables a single communications channel to carry simultaneously data transmissions from multiple sources without any extra cable. DWDM uses different wavelengths to carry separate streams of data over the same cable at the same time. Prior to DWDM, optical networks could use only a single wavelength per strand.

Synchronous optical network (SONET) is popular in transmitting voice, data, and video over optical networks. Most long-distance telephone systems in the world use SONET to standardize and connect multiple and different long-distance carriers. The goals of SONET are to (1) interwork the multiple carriers with a common signaling standard regarding wavelength, timing, and framing structures, (2) unify the pulse code modulation (PCM) channels, which are incompatible with each other, (3) multiplex different digital channels with different speed in terms of data rates, and (4) provide support for operations, administration, and maintenance systems. SONET is a synchronous system, meaning that the sender and receiver are tied to a common clock, whereas asynchronous transfer mode (ATM) system is not tied to a common clock because it permits irregular cell arrivals. SONET operates at the physical layer of the ISO/OSI model and supports gigabit transmission rates. SONET has a fault tolerance mechanism (i.e., redundancy) in that it has a backup ring to ensure continued transmission if the primary ring fails.

(Y) Body Area Networks Body area network is a technology that allows communication between ultra-small and ultra-low-power intelligent sensors/devices that are located on the body surface or implanted inside the body. In addition, the wearable/implantable nodes can also communicate to a controller device that is located in the vicinity of the body. These radio-enabled sensors can be used to continuously gather a variety of important health and/or physiological data (i.e., information critical to providing health care) wirelessly.

Radio-enabled implantable medical devices offer a revolutionary set of possible applications, including smart pills for precision drug delivery, intelligent endoscope capsules, glucose monitors, and eye pressure sensing systems. Similarly, wearable sensors allow for various medical and physiological monitoring (e.g., electrocardiogram, temperature, respiration, heart rate, and blood pressure) and disability assistance.

(z) Radio Frequency Identification Networks Radio frequency identification (RFID) network systems share information across organizational boundaries, such as *supply chain applications.* RFID systems provide a method for tracking the movement of goods throughout the supply chain. These systems use small tags with embedded microchips containing data about an item and its location to transmit radio signals over a short distance to special RFID readers. These readers then pass the data over a network to a computer for processing the tag's data. These tags, unlike bar codes, do not need LOS contact to be read. RFID systems can be very complex, and implementations vary greatly across industries and organizations.

An RFID system is composed of three components such as an RF subsystem, an enterprise subsystem, and an inter-enterprise subsystem. The four major categories of RFID risk are (1) business process risk (loss of critical and operational records and cloning of tags), (2) business intelligence risk (access to sensitive or proprietary information), (3) privacy risk (profiling individuals using the tagged items), and (4) externality risk (health hazards from electromagnetic radiation).

(ii) Network Connections

Network connections consist of connectivity hardware devices and software to share resources and information among the networks. This would enable a network user to establish a communication link with a user from another network, and vice versa. These hardware devices and software move data frames and packets from one cable segment to another. They may use a piggybacking technique of temporarily delaying outgoing acknowledgements of data frames so that they can be attached to the next outgoing data frames.

In this section, we discuss various types of network connectivity hardware devices and software such as network switches, bridges, brouters, repeaters, gateways, proxies and reverse proxies, modems, port protection devices, multiplexers, hardware controllers, protocol converters, protocol analyzers, backbone networks, concentrators, hubs, connectors, NICs, front-end processors, network nodes, sockets, ports, subnets, portals, wireless devices such as smart phones, personal digital assistants (PDAs), and Bluetooth; wireless access points, domain controller, and programmable logic controller. In addition, measurement metrics such as quality of service (QoS) and quality of protection (QoP) are addressed to improve network performance.

Although firewalls, routers, sensors, and hardware/software guards are classified as a part of network connections, we discussed them in system security section of this Domain due to their dual functionality and the fact they have greater security implications than network connectivity.

(A) Network Switches A computer network has three main components: computers, links, and switches. The web of links and switches carry data between the computers. Links are made of copper (either twisted pair or coaxial cable) or fiber optics. Transmission equipment at each end of the fiber or copper generates the electrical or optical signals. There are also satellite and microwave links that send radio waves through the air. Fiber optics has several advantages over other types of links—most notably its very high bandwidth.

As the information travels through the network, the switches decide which link it will have to traverse next in order to reach its destination. The rules by which the switches and the users' computers coordinate the transmission of information through the network are called protocols.

Bridges and repeaters share the same physical transmission medium to interconnect or extend a local-area network (LAN). Switches and hardware devices are designed for the opposite purpose of bridges and repeaters. Switches, in the form of routers, interconnect when the systems forming one workgroup are physically separated from the systems forming other workgroups. Switches do not extend LANs as bridges and repeaters do. Switches are primarily used to (1) implement multiple, parallel transmission medium segments to which different groups of workstations can be connected, and (2) provide full network bandwidth to multiple groups of systems.

Network switches are devices that provide connectivity between two or more hosts located on the same network segment. They are similar to hubs in that they allow communications between hosts, but, unlike hubs, the switches have more intelligence and send communications to only those hosts to which the communications are addressed. The benefit of this from a security standpoint is that when switches are employed on a network, it is much more difficult to eavesdrop on communications between other hosts on the network segment. This is extremely important when a Web server is on a network segment that is used by other hosts. For example, if a hub is used and a host on the DMZ is compromised, an attacker may be able to eavesdrop on the communications of other hosts on the DMZ, possibly leading to the compromise of those hosts or the information they communicate across the network. For example, e-mail servers in their default configurations receive unencrypted passwords; a compromise of the Web server would lead to the exposure of e-mail passwords by sniffing them from the compromised Web server.

Switches can have a negative impact on network-based intrusion detection and prevention systems (IDPSs). Most network switches allow network administrators to configure a specific port on the switch, known as a span port, so that it replicates the entire switch's traffic to the port used by the IDPS. This allows a network-based IDPS to see all traffic on a particular network segment. However, under high loads, the switch might have to stop sending traffic to the span port, causing the IDPS to be unable to monitor network activity. Also, other devices use span ports, and there are typically very few span ports on a switch; therefore, it might not be possible to connect an IDPS to a particular switch because its span ports are all in use.

WHAT ARE THE FUNCTIONS OF BRIDGES, ROUTERS, REPEATERS, AND SWITCHES?

- Bridges are generally considered to be faster than routers since the processing they perform is simpler.
- Routers are limited to particular routing protocols, while bridges may be transparent to most routing protocols.

- Bridging protocols are semi-automatic. Routers are automatic and depend on routing tables which typically must be maintained.
- Bridge protocols limit the size of any extended LAN network while routers do not. Routers are used to connect LANs, WANs, and WANs.
- Routers do not propagate broadcast. Bridges do.
- Bridges and repeaters share the same physical transmission medium to interconnect or extend a LAN
- Switches do not extend LANS as bridges and repeaters do.
- Routers and switches provide the simplest method of local authentication for network infrastructure devices.
- Repeaters and hubs are similar in function.
- Bridges and switches are similar in function.

(B) Bridges A bridge is a device that connects similar or dissimilar two or more LANs together to form an extended LAN. Bridges are protocol independent devices and are designed to store and then forward frames destined for another LAN. Bridges are transparent to the end-stations connecting through the bridge. Bridges can reduce total traffic on the extended LAN by filtering unnecessary traffic from the overall network. A bridge functions in a MAC/Data Link layer of the ISO/OSI Reference Model. Bridges are similar to switches. Next, various types of bridges are discussed briefly.

Local bridges connect to LANs together directly at one bridge. **Remote bridges** connect two distant LANs through a long distance circuit, which is invisible to the stations on the LANs.

Learning bridges learn whether they must forward packets by observing the source addresses of packets on the networks to which they are connected. The bridge maintains a table of source addresses for each sub-network. Learning bridges generally participate in a *spanning tree algorithm*, in which the bridges communicate with each other to establish a tree through the extended LAN so that there is one and only one path between any two stations, preventing endlessly circulating packets. The spanning tree algorithm is used to build plug-and-play bridges.

With **source routing bridges**, the source and destination stations explicitly participate in the routing through the bridges. The source station inserts the route through the bridges to the information field of the packet. The bridge, in turn, just uses the routing information supplied by the source station to route packets.

Bridges and routers are lower-level network interconnection devices. Typically network interconnection strategies will involve some combination of bridges and routers. The decision when to use a bridge and when to use a router is a difficult one. Enterprises may use bridging to connect LANs between different buildings on corporate or university campuses. Bridging access point (AP) devices are typically placed on top of buildings to achieve greater antenna reception.

(C) Brouters Brouters are routers that can also bridge; they route one or more protocols and bridge all other network traffic. Routing bridges are those capable of maintaining the protocol transparency of a standard bridge while also making intelligent path selections,

just like a router. Brouters merge the capabilities of bridges and routers into a single, multi-functional device.

(D) Repeaters Repeaters offer the simplest form of inter-connectivity hardware devices. Multiple cables can be connected by repeaters to make larger networks. They merely generate or repeat data packets or electrical signals between cable segments. Repeaters perform data insertion and reception functions. They receive a message, amplify it, and then retransmit it, regenerating the signal at its original strength in both directions. In their purest form, repeaters physically extend a network. They also provide a level of fault tolerance by isolating networks electrically, so problems on one cable segment do not affect other segments. However, repeaters exert stress on a network's bandwidth due to difficulty in isolating network traffic. Repeaters are independent of protocols and media. A repeater operates in a Physical Layer of the ISO/OSI Reference Model and performs no Data Link Level functions. Repeaters are similar to hubs.

(E) Gateways A gateway is an interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. In general, a gateway is a device that connects incompatible networks using different communications protocols so that information can be passed from one to the other (i.e., two connection-oriented protocol such as TCP/IP and ATM transport protocol). A gateway transfers information and converts it to a form compatible with the receiving network's protocols (e.g., an e-mail gateway could translate the Internet messages into short messaging system (SMS) messages for mobile phones). Several types of gateway exist, including data gateways, e-mail gateways, application gateways, secure gateways, XML gateways, and VPN gateways.

WHICH CONNECTIVITY DEVICE OPERATES WHERE IN THE OPEN SYSTEM INTERCONNECTION LAYER?

- A gateway operates in the application layer and transport layer.
- A router operates in the network layer.
- A bridge and switch operates in the data-link layer.
- A repeater and hub operates in the physical layer.
- A NIC operates at the data-link layer.
- Firewalls operate at lower layers and higher layers of the ISO/OSI model. Basic firewalls operate on one or a few lower layers while more advanced firewalls examine all of the layers. Firewalls that examine more layers can perform more granular and thorough examinations. A firewall that handles lower layers only (e.g., data-link layer) cannot usually identify specific users.

(F) Proxies and Reverse Proxies A **proxy** is a computer with software acting as a barrier between a private network and the Internet by presenting only a single network address to external sites. By acting as a go-between representing all internal computers, the Web proxy protects network identities while still providing access to the Internet. Proxy servers forward application traffic through a firewall. Proxies tend to be specific to the protocol they are designed to forward and may provide increased access control or audit. A proxy server is a firewall component that manages Internet traffic to and from a LAN. The proxy server also provides document caching and access control. A proxy server can improve performance by supplying frequently requested data (e.g., a popular Web page) and can filter and discard requests that the owner does not consider appropriate (e.g., unauthorized access requests).

Reverse proxies are devices that sit between a Web server and the server's clients. The term "reverse proxy" is used because the data flow is the reverse of a traditional (forward) proxy. Reverse proxies can serve as a valuable addition to the security of a Web server. The term is used rather loosely in the industry and can include some or all of these functionalities:

- Encryption accelerators, which offload the computationally expensive processing required for initiating SSL/TLS connections
- Security gateways, which monitor HTTP traffic to and from the Web server for potential attacks and take action as necessary, acting in essence as an application level firewall
- Content filters, which can monitor traffic to and from the Web server for potentially sensitive or inappropriate data and take action as necessary
- Authentication gateways, which authenticate users via a variety of authentication mechanisms and control access to URLs hosted on the Web server itself

Reverse proxies should be considered for any high-risk Web server deployment. While they do add risk by requiring the deployment of additional hardware and software, the risk is generally outweighed by the benefits. In addition to the functionality just listed, Web proxies are valuable because they add an additional layer between a Web server and its less trusted users. Due to their highly specialized nature, proxies are easier to secure than Web servers. Proxies also further obfuscate a Web server's configuration, type, location, and other details that are pertinent to attackers. For example, Web servers have banners that frequently reveal the Web server type and version, and these banners sometimes cannot be changed. With a reverse proxy, this is not an issue because the proxy can rewrite the banner before it is sent to users.

(G) Modems If computers are connected over long distances, modems are needed. The term "modem" is an acronym for *mo*dulator and *dem*odulator. It is a device that modulates and demodulates signals. Modems are primarily used for converting digital signals into quasi-analog signals for transmission over analog communication channels and for reconverting the quasi-analog signals into digital signals. Many additional functions may be added to a modem to provide customer service and control features. Modems can be installed either internally or externally to a computer.

The range of options available on modems is quite large. Simple units do little more than perform the digital-to-analog signal conversion, but more intelligent units can automatically dial phone numbers, store messages for delayed transmission, and perform a number of other functions.

These factors should be considered in modem selection:

- The requirements of the communications software and target computer
- Speed (measured in baud)
- Physical connection (RS-232 and V.35)
- Duplex (full or half)
- Synchronization scheme (asynchronous or synchronous)
- Dialing (manual or automated)

Basic modems have two major uses: They are attached a to stand-alone PC either internally or externally, and they are attached to network-based PCs. Other modems include cable and digital modems.

A **cable modem** provides high-speed access to the Internet. Its drawbacks include inadequate security due to shared media, such as coaxial trunks, and lower throughput due to several users using the service at the same time. Some cable data providers offer limited firewall protection and packet filtering services, where the latter is meant to protect against broadcasts.

A **digital modem** provides high-speed access to the Internet with XDSL constantly connected with the fixed IP address, which is less vulnerable to attacks than dial-up lines.

(H) Port Protection Devices A **port protection device (PPD)** is fitted to a communications port of a host computer and authorizes access to the port itself, prior to and independent of the computer's own access control functions. A PPD can be a separate device in the communications stream (typically PPDs are found only in serial communications streams), or it may be incorporated into a communications device (e.g., a modem). PPDs typically require a separate authenticator, such as a password, in order to access the communications port.

One of the most common PPDs is the dial-back modem. In a typical dial-back modem sequence, a user calls the dial-back modem and enters a password. The modem hangs up on the user and performs a table look-up for the password provided. If the password is found, the modem places a return call to the user (at a previously specified number) to initiate the session. The return call itself also helps to protect against the use of lost or compromised accounts. This is, however, not always the case. Malicious hackers can use the call forwarding feature, to reroute calls. Another device is a terminal server that acts as a PPD for remote maintenance connections, such as router maintenance ports.

(I) Multiplexers A multiplexer is a device for combining two or more channels. A channel is a single path provided from a transmission medium either by physical separation (e.g., cable) or by electrical separation (e.g., frequency- or time-division multiplexing). In optical communications, wavelength-division multiplexing (WDM) involves the use of several distinct optical sources (e.g., lasers) with each having a distinct center frequency. In general, multiplexing is the combining of two or more information channels onto a common transmission medium.

(J) Hardware Controllers A controller is a hardware device that coordinates and manages the operation of one or more I/O devices, such as computer terminals, workstations, disks, and printers. It synchronizes the operations of these devices with the operation of the computer system as a whole. A controller organizes a series of actions from requests received from computer terminals, other controllers, or host computer systems. Many varieties of controllers exist, including communication controller, store controller, cluster controller, and terminal controller.

A **communication controller** manages the details of communication line control and the routing of data and messages through a network in which a series of computer programs are stored and executed. A **store controller** is a programmable unit in a network used to collect data, direct inquiries, and control communication within a computer system. It stores information such as tables, lists, and control blocks used by the host processor to work with the store controller. A **cluster controller** is a device that controls the I/O operations of more than one device connected to it through a series of computer programs stored and executed in the unit. A **terminal controller** is used in WANs in accessing mainframe computers.

(K) Protocol Converters **Protocol converters** are devices that change one type of coded data to another type of coded data for computer processing. Conversion facilities allow an application system conforming to one network architecture to communicate with an application system conforming to some other network architecture.

(L) Protocol Analyzers **Protocol analyzers** vary widely in functions and user friendliness. Examples of their functions include password sniffing and packet sniffing performed by sniffers. Protocol analyzers perform password sniffing to capture passwords for unauthorized reuse.

Sniffers are LAN protocol analyzers that capture packets and analyze them for certain attributes. They capture illegally short or long frames typically discarded by standard LAN adapters. Sniffers are programs to capture, interpret, and store packets traversing a network used for later analysis and debugging network problems. Sensitive data, such as a username (user ID) and password combination, confidential e-mail messages, and file transfers of proprietary data can be sniffed.

The protocol analyzer allows the LAN administrator to see what is happening on the LAN in real time and observe problems as they occur. It is a valuable tool for online testing of service degradation.

(M) Backbone Network A **backbone network** is a central network to which other networks connect. Users are not attached directly to a backbone network; they are connected to the access networks, which in turn connect to the backbone. A backbone network provides connection between LANs and WANs. Dumb terminals can be attached directly to the backbone through terminal servers. The backbone network is a high-speed connection within a network that connects shorter, usually slower circuits.

HOW DO NETWORKS GET CONNECTED?

- Front-end networks connect workstations and servers for file sharing and application processing.
- Back-end networks connect peripherals, such as disk drives and high-speed printers.
- A backbone network is a central network to which other networks connect.

(N) Concentrators The major function of **concentrators** is to gather together several lines in one central location. Concentrators are the foundation of a Fiber Distributed Data Interface (FDDI) network and are attached directly to the FDDI dual ring. Concentrators provide highly fault-tolerant connections to the FDDI rings.

The concentrator allows stations to be inserted and removed with minimal effect on the operation of the ring. One function of the concentrator is to ensure ports (stations) are automatically bypassed in response to a detected fault connection, a high error rate, or when a user powers down the station. This bypass function of the concentrator enhances the reliability of the FDDI ring.

(O) Hubs A **hub** can be thought of a central place from which all connecting lines are made. All the lines coming into a hub must operate at the same speed. Hubs do not amplify the incoming signals, unlike repeaters. Like repeaters, hubs do not examine IEEE 802 addresses. If two frames arrive at the same time, they will collide, as with a coaxial cable. Hubs are similar to repeaters.

There are a number of definitions of the term "hub," including:

The link from remote end users to the central satellite and back to the central satellite dish

The link from Ethernet LANs to host computers

Another name for the Ethernet concentrator

Although hubs are cheaper than switches, hubs are becoming obsolete due to falling prices of switches and due to better performance of switches over hubs. However, legacy hubs still exist. The backbone network was also used as a hub, but it is not common now.

(P) Connectors A **connector** is an electro-mechanical device on the ends of cables that permit them to be connected with, and disconnected from, other cables. For example, connectors join controllers to peripherals (e.g., printers and hard disk drive) and computers. The type of cable used determines the type of connector needed (e.g., a thicknet coaxial cable needs Type N connector).

(Q) Network Interface Cards **(NICs)** are circuit boards used to transmit and receive commands and messages between a PC and a LAN. They are expansion cards, and they mediate between the computer and the physical media (e.g., cable) over which transmissions take place. When the NIC fails, workstations and file servers also fail. **Network adapters**, functioning similarly to NICs, establish a connection to other computers or peripherals, such as a printer in the network. NICs operate at the data-link layer.

Mobile wireless stations need an add-on card called a wireless NIC with a built-in radio and antenna signals to establish connections to the wireless LAN. In a wireless LAN, a station or client can be a laptop/notebook/desktop computer or PDA with a wireless NIC. Usually the wireless NIC is inserted in the client's personal computer memory card international association (PCMCIA) slot or universal serial bus (USB) port.

(R) Front-End Processors A **front-end processor (FEP)** is a programmed logic or stored program device that interfaces data communication equipment with an I/O bus or the memory of a data processing computer. It reduces the workload of a host computer by performing certain tasks that the host computer would otherwise do. A programmable FEP (PFEP) puts less demand on the host computer by sharing some tasks with the host. The PFEP performs polling, code conversion, and data formatting functions.

(S) Network Nodes The term "network node" (or "network node") has multiple definitions:

A physical connection (junction) point where communication lines come to and leave from

The point at an end of a branch

The representation of a state or event in terms of a point on a diagram

In network topology, it is a terminal of any branch of a network or an interconnection common to two or more branches of a network.

In a tree structure, it is a point at which subordinate items of data originate.

In a switched network, it is one of the switches forming the network backbone.

Nodes can be distributed to host processors, communication controllers, or terminals. Nodes are labeled as major, minor, endpoint, host, master, intermediate, or terminal.

WHICH NETWORK USES WHAT TOPOLOGY?

Topology affects security, so proper selection and functioning of topology is important to ensure proper security. Several types of topologies exist for several networks.

Star topology. All nodes are connected to a single central hub. Traffic is in both directions.

Bus topology. All nodes are connected to a central cable, called the bus or backbone. Traffic is in both directions.

Ring topology. All nodes are connected to one another in the shape of a closed loop, so that each node is connected directly to two other nodes, one on either side of it. Traffic is in one direction.

Mesh topology. Networked components are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.

Hybrid topology. A linear bus backbone connects with the star-configured network.

Dial-up telephone services and PBX systems use the star topology.

Ethernet mostly uses the bus topology.

FDDI uses the ring topology.

The Internet uses the mesh topology.

(T) Sockets Sockets are end points created in a TCP service by both the sender and the receiver. Each socket has a socket number consisting of the IP address of the host and a port number. For a TCP service to be obtained, a connection must be made between a socket on the sending computer and a socket on the receiving computer. Two or more connections can terminate at the same socket. Connections are identified by the socket number at both ends, and no virtual circuit numbers are used. In TCP/IP, the socket number is the concatenation of the sender's or receiver's IP address and the port number for the service being used. The pair of these sender's and receiver's socket numbers uniquely specifies the connection to the Internet.

(U) Ports The term "port" has multiple definitions.

An access point for data entry or exit

A connector on a device to which cables for other devices such as terminals and printers are attached

In a communication network, it is a point at which signals can enter or leave the network en route to or from another network.

A port is identified by a port number assigned either ephemerally or permanently to enable IP packets to be sent to a particular process on a computer connected to the Internet. An ephemeral port number goes out of use when the session ends. All ports should be closed when they are not in use because open and unused ports invite attackers.

Some protocols such as file transfer protocol (FTP) and simple mail transfer protocol (SMTP) use the same permanent port number in all TCP/IP implementations. Note that some connections use TCP protocol for FTP, SMTP, and TELNET services; some use user datagram protocol (UDP) protocol for domain name system (DNS) service; and while others use either TCP or UDP for Packet Internet groper (PING) echo service.

Telnet is the TCP/IP standard network virtual terminal protocol that is used for remote terminal connection service and that allows a user at one site to interact with systems at other sites as if that user terminal were directly connected to computers at those sites.

PING is a TCP/IP diagnostic program that sends one or a series of Internet Control Message Protocol (ICMP) echo packets to a user-specified IP address. The echo packet requests the receiver

to reply with an echo reply packet. The PING program measures and displays the round-trip time for replies to return, the number of hosts that are operational, the number of IP addresses that are valid, and the percentage of returned packets or lost packets. The PING protocol tests the ability of a computer to communicate with a remote computer by sending a query and receiving a confirmation response.

There are a number of ports, including serial, parallel, terminal, I/O, protocol, disabled, and communication ports. Ports should be closed when not in use because open ports invite attackers.

(V) Subnets There are a number of definitions for the term "subnet" (also called subnetwork):

A network that forms part of a larger network

A group of nodes with the same network ID

The Ethernet part of a main network

In TCP/IP, it is a part of a network that is identified by a portion of the Internet address.

In terms of the ISO/OSI Reference Model, the subnet comprises the layers below the transport layer (i.e., the network, data-link, and physical layers). The network layer operates ATM networks, ad hoc networks, P2P networks, and WANs. The medium access control sublayer of the data-link layer operates wired LANs and MANs, wireless LANs and MANs, and virtual LANs. The physical layer operates ISDN,PSTN, and SONET.

The application layer operates the Internet (wired web and wireless web), client/server network, content delivery network, and VoIP network. There are no networks operating either at the transport layer or at the session layer because the transport layer provides an understanding of layered protocols and end-to-end connection-oriented services, and the session layer provides services such as dialog control and token management.

The WAN machines are called host computers, which are connected by a communications subnet or simply subnet. Individual customers own the host (personal) computers whereas the telephone company or the ISPs own and operate the subnets. In most WAN networks, the subnet consists of two distinct components: transmission lines to move bits between machines and switching elements, which are special computers (routers) that connect three or more transmission lines.

All host computers in a main network must have the same network number to the outside world. Since the IP addresses are limited in supply, the subnets are created by splitting the main network into several parts for internal use with different IP addresses, but they still act like a single network to the outside world. Hence, the subnets are not visible to the outside the world.

In an IP address, a subnet address is an extension that allows users in a network to use a single IP network address for multiple physical subnetworks. To implement subnetworking, the main router needs a subnet mask that indicates the split among network, subnet, and host. To accomplish this, routing tables need to be changed to add new entries of subnets.

Subnets face traffic congestion problems for packets (e.g., increased delay and decreased throughput) and QoS issues. Some solutions to handle the congestion problems include:

- Increasing the resources.
- Decreasing the load.

- Designing open-loop and closed-loop controls.
- Establishing caching policy, retransmission policy, and flow control policy, where discarded or choked packets are retransmitted or sent back or the load can be reduced

Some methods to improve QoS include:

- Buffering at the client side.
- Increasing the router capacity.
- Traffic shaping.
- Resource reservation.
- Packet scheduling.

(W) Portals A **portal** is a Web site that acts as a gateway to the Internet. It is a collection of links, content, and services designed to guide end users for information search on the Internet (e.g., Yahoo and MSN). A portal is a server that offers access to one or more applications through a single centralized interface. Most portals are Web based—for them, the portal client is a regular Web browser. The application client software is installed on the portal server, and it communicates with application server software on servers within the organization. The portal server communicates securely with the portal client as needed; the exact nature of this communication depends on the type of portal solution in use.

Examples of portals include:

- Application portals, such as an secure socket layer (SSL) portal
- VPN, which is a Web-based portal providing a user with access to multiple Web-based applications from a single portal Web site
- An Ethernet portal connected to the Internet
- Mobile (wireless) portals that provide content and services on users' mobile devices

(X) Wireless Devices The most frequently used handheld wireless devices include PDAs, text-messaging devices, smart phones, and Bluetooth.

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. They offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a PC through a cable or wireless transmission. Newer versions of PDAs allow users to download their e-mail, connect to the Internet, and one-way or two-way text-messaging devices. **Text-messaging** technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld device via the Internet and wireless network. Mobile phones with information-processing and data networking capabilities are called **smart phones**.

Bluetooth is a popular ad hoc network standard, which describes how mobile phones, computers, and PDAs should interconnect with each other, with home/business phones, and with computers using short-range wireless connections. Bluetooth network applications include

wireless synchronization; e-mail, Internet, and intranet access using local PC connections; hidden computing through automated applications and networking; and applications that can be used for hands-free devices.

Security Concerns over Cell Phones and PDAs Mobile handheld devices (e.g., cell/mobile phones and PDAs) typically lack a number of important security features commonly found on desktop computers. They also lie at the periphery of an organization's infrastructure, which can make them difficult to administer centrally. Once the threats are understood, individuals and organizations aware of the potential risks involved can often mitigate many of the associated threats with add-on security mechanisms and other safeguards.

Security threats to mobile handheld devices are listed next.

- Application development in terms of cross-platform development and testing
- Loss, theft, or disposal of devices
- Unauthorized access in terms of bypassing the authentication mechanisms
- Malware through Internet downloads, messaging services, and Bluetooth connections
- Spam in terms of unwanted text messages, phishing, and DoS
- Electronic eavesdropping through spy software
- Electronic tracking through an online SMS gateway
- Cloning using electronic serial number (ESN) and mobile identification number (MIN)
- Server-resident data such as e-mail, address book, photos, and voice-mail

Safeguards over Cell Phones and PDAs Safeguards over cell phone and PDAs are organized in terms of user-oriented measures and organizational-oriented measures.

User-Oriented Measures Maintaining the security of a handheld device involves the active participation of the user. Users should be instructed about procedures to follow and precautions to take when using organization devices.

User-oriented measures are listed next.

- Maintaining physical control over mobile handheld devices
- Enabling user authentication with passwords and PINs
- Backing up data on desktop computers and/or memory cards
- Protecting sensitive data on a device with encryption
- Protecting from malicious programs
- Curbing wireless interfaces by turning off Bluetooth, Wi-Fi, infrared, and other wireless interfaces until needed (This is particularly important for Bluetooth devices due to the increased risk of encountering mobile malware in crowded settings, such as airports, sports events, or concerts. Being invisible prevents the device from being scanned and located and its wireless interface from being used as an avenue of attack. Disabling a wireless interface also extends the battery life of the device.)

Specific user-oriented measures include:

- Deactivating compromised devices.
- Minimizing functionality.
- Adding prevention and detection software.

Organizational-Oriented Measures If not addressed properly, handheld devices have the potential to create a security weakness in an organization's security infrastructure. For example, employees who buy their own units may attempt to synchronize them with an office workstation or use their workstation connectivity to access the organization's intranet. A device with wireless capabilities could potentially create an unauthorized side channel to the Internet. These devices contain sufficient memory to hold a significant amount of an organization's data for working away from the office while on travel or at home, and these data need to be protected.

Specific organizational-oriented measures include:

- Establishing a mobile device security policy.
- Preparing deployment and operational plans.
- Performing risk assessment and management.
- Instilling security awareness through training.
- Performing configuration control and management.

Bluetooth Devices Bluetooth is a very popular ad hoc network standard. In Bluetooth technology, no fixed infrastructure, such as base stations or access points, exists. In ad hoc networks, devices maintain random network configurations formed on the fly, relying on a system of mobile routers connected by wireless links that enable devices to communicate with each other. Devices within an ad hoc network control the network configuration, and they maintain and share resources. Ad hoc networks are similar to P2P networking in that they both use decentralized networking, in which the information is maintained at the end user location rather than in a centralized database. However, ad hoc and P2P networks differ in that P2P networks rely on a routing mechanism to direct information queries, whereas ad hoc networks rely on the device hardware to request and share the information.

Ad hoc networks allow devices to access wireless applications, such as address book synchronization and file-sharing applications, within a WPAN. When combined with other technologies, these networks can be expanded to include network and Internet access. Bluetooth devices that typically do not have access to network resources but that are connected to a Bluetooth network with an 802.11-capable device can achieve connection within the corporate network as well as reach out to the Internet.

Ad hoc networks are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It is touted as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a WPAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices eliminate the need for cables and provide a bridge to existing networks.

Major Problems in Bluetooth Security Major problems with the Bluetooth standard security features are listed next.

- **Strength of the challenge-response pseudo-random generator is not known.** The random number generator may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
- **Short PINs are allowed.** Weak PINs that are used for the generation of link and encryption keys can be guessed easily. Increasing the PIN length in general increases the security.
- **No elegant way to generate and distribute PINs exists.** Establishing PINs in large Bluetooth networks with many users may be difficult. Scalability problems frequently yield security problems.
- **Encryption key length is negotiable.** Standards need to be developed for a more robust initialization key generation procedure with a minimum key length.
- **The master key is shared, and the unit key is reusable and becomes public once used.** Standards need to be developed for a better broadcast-keying scheme. Use a unit key as input to generate a random key. Use a key set instead of only one unit key.
- **No user authentication exists.** Only device authentication is provided. Application-level security and user authentication can be employed.
- **Authentication attempts are unlimited.** The Bluetooth specification requires a time-out period between repeated attempts that will increase exponentially.
- **Key length is negotiable.** A global agreement must be established on minimum key length.
- **Unit key sharing can lead to eavesdropping.** A corrupt user may be able to compromise the security between (gain unauthorized access to) two other users if that corrupt user has communicated with either of the other two users. This is because the link key (unit key) derived from shared information is disclosed.
- **Privacy may be compromised if the Bluetooth device address is captured and associated with a particular user.** One the device address is associated with a particular user, that user's activities could be logged, resulting in a loss of privacy.
- **Device authentication is simple shared-key challenge-response.** One-way-only challenge-response authentication is subject to MitM attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
- **End-to-end security is not performed.** Only individual links are encrypted and authenticated. Data are decrypted at intermediate points. Applications software above the Bluetooth software can be developed.
- **Security services are limited.** Audit, nonrepudiation, and other services do not exist. If needed, these can be developed at particular points in a Bluetooth network.

Countermeasures for Bluetooth Security Problems Countermeasures include management, operational, and technical countermeasures.

- **Management countermeasures.** The first line of defense is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth-enabled devices. Organizations using Bluetooth technology need to establish and document security policies that address the use of Bluetooth-enabled devices and the users' responsibilities. The

policy document should include a list of approved uses for Bluetooth networks, the type of information that may be transferred in the network, and any disciplinary actions that may result from misuse. The security policy should also specify a proper password usage scheme.

- **Operational countermeasures.** Since Bluetooth devices do not register when they join a network, they are invisible to network administration. Consequently, it is difficult for administrators to apply traditional physical security measures. However, some security approaches can be applied, including establishing spatial distance and securing the gateway Bluetooth devices that connect remote Bluetooth networks or devices.

  Establishing spatial distance requires setting the power requirements low enough to prevent a device operating on the organization's premises from having sufficient power to be detected outside a physical area (e.g., outside the office building). This spatial distance (30 feet) in effect creates a more secure perimeter.

- **Technical countermeasures.** As with WLANs, Bluetooth technical countermeasures fall into one of two categories: software security solutions and hardware security solutions. Bluetooth software solutions focus on PIN and private authentication, while hardware solutions involve the use of the Bluetooth device address and link keys (128-bit unit keys) that reside at the link level. Bluetooth PINs operate at the link level with a fixed PIN, which is a weak security procedure.

Specific controls over Bluetooth security are listed next.

- Implement Bluetooth device authentication as an extra layer of security. Incorporating application-level software that requires password authentication to secure the device will add an extra layer of security.
- Implement a hardware solution, such as frequency-hopping schemes, which allow devices to communicate even in areas where a great deal of electromagnetic interference occurs. Frequency-hopping schemes also offer protection from burst errors by continually moving signals in and out of the inference band and by making bit error corrections by using forward error correction. Frequency hopping provides only minimal protection and should not be relied on by itself.
- Implement a hardware solution, such as voice authentication (biometrics) as a part of a multifactor authentication. Voice authentication can help organizations prevent malicious users from compromising remote Bluetooth devices and networks. The hosting devices of Bluetooth devices and networks should be secured in the same manner as PDAs, cell phones, WLANs, and related devices.
- Consider a trusted third party (TTP) authentication. TTP centralizes authentication, and as long as the TTP remains secure and trusted, the trustworthiness of the devices is not a concern. Centralized key management authority, which is similar to TTP authentication, is another possibility. Centralized key management, unlike TTP, maintains and distributes keys, so that only trusted devices have access to the secure keys.

(Y) Wireless Access Points Wireless access points (APs) are devices that act as conduits to connect wireless communication devices together to allow them to communicate and create a wireless network. For example, employees traveling on business work with wireless-enabled devices can connect to an organization's network via any one of the many public Internet access points or public hot spots.

The two fundamental types of WLAN components are client devices (e.g., computers, PDAs, and smart phones) and access points, where the latter logically connect client devices with a distribution system (DS), which is typically an organization's wired network infrastructure. The DS is the means by which client devices can communicate with the organization's wired LANs and external networks, such as the Internet. Some WLANs also use wireless switches, which act as intermediaries between APs and the DS. The purpose of the wireless switch is to assist network administrators in managing the WLAN infrastructure. The security of each of the WLAN components, including client devices, APs, and wireless switches, is heavily dependent on its WLAN security configuration.

The AP, which acts a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface (e.g., IEEE 802.3), and bridging software. The AP functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network.

APs generally have only three encryption settings available: none, 40-bit shared key, and 104-bit setting. The setting of "none" represents the most serious risk since unencrypted data traversing the network can easily be intercepted, read, and altered. A 40-bit shared key will encrypt the network communications data, but there is still a risk of compromise (broken by brute-force attack using a high-end graphics computer or even a low-end computer). In general, 104-bit encryption is more secure than 40-bit encryption because of the significant difference in the size of the cryptographic keyspace.

Attackers can introduce rogue devices and create rogue APs to conduct their attacks. A rogue device is an unauthorized node on a network; a rogue AP is an unauthorized entry point.

Some examples of attacks using wireless vulnerabilities are listed next.

- Passive attacks include eavesdropping and traffic analysis.
- Active attacks include masquerading, replay, message modification, DoS, and misappropriation of assets.

  The deployment of rogue WLAN devices is a form of active attack. For example, an attacker deploys an AP that has been configured to appear as part of an organization's WLAN infrastructure. This can provide a backdoor into the wired network, bypassing perimeter security mechanisms, such as firewalls. In addition, if client devices inadvertently connect to the rogue AP, the attacker can view and manipulate communications on the client devices (i.e., conducting a MitM attack) and potentially gain access to the client devices themselves.
- In a dual-connect scenario when a wireless network is connected to the wired network, an attacker exploits insecure laptop configurations to gain unauthorized access to an organization's core network.
- Wireless MitM attacks use an insecure laptop configuration to intercept or alter information transmitted wirelessly between the target laptop and a wireless access point
- Attacks on smart phones can involve stealing data or injecting malicious code using phone memory cards.

Some examples of security controls to mitigate wireless vulnerabilities are listed next.

- Users should use a personal firewall when accessing public wireless networks in airports and conference centers.

- Obtain vendor upgrades to software and firmware.
- Install a VPN to stop leakage of data through hot spots because a VPN can encrypt the data transmitted in public places,
- Install personal firewalls in public places, where possible.
- Establish proper configuration settings.
- Incorporate wireless and mobile device security component topics in training.
- Implement handheld scanner or network authentication mechanisms to detect rogue wireless client devices.
- Install a wireless intrusion detection system (WIDS) to continuously monitor, detect, and respond to malicious activities before they inflict damage. Use of WIDS is better than using handheld scanners or network authentication mechanisms to find rogue APs.

The detection capabilities of WLAN monitoring tools are listed next.

- Unauthorized WLAN devices (rogue devices), including rogue APs and unauthorized client devices
- WLAN devices that are misconfigured or using weak WLAN protocols and protocol implementations
- Unusual WLAN usage patterns (e.g., extremely high number of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLANs in a short period of time)
- DoS attacks and conditions (e.g., network interference). (For example, a large number of events involving the termination of WLAN services can indicate a DoS attack.)
- Impersonation and MitM attacks. (For example, some WIDS sensors can detect when a device is attempting to spoof the identity of another device.)

Organizations should be able to identify the physical location of a detected WLAN threat by using triangulation, which involves estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be the estimated distance from each sensor. This method allows an organization to send physical security staff to the location to handle the threat.

(Z) Domain Controller A **domain controller** is a server responsible for managing domain information, such as login identification and passwords.

(AA) Programmable Logic Controller A **programmable logic controller (PLC)**, used in industrial control systems, is a programmable microprocessor-based device designed to control and monitor various inputs and outputs used to automate industrial processes. Since a PLC is a first-level decision-making device controlling safety interlocks, it can become a single point of failure.

(BB) Quality of Service and Quality of Protection Network congestion occurs when too many network packets are present in the subnet (i.e., too much traffic), thus degrading the network performance in terms of some lost packets or all packets undelivered. The presence of congestion means that

the load is temporarily greater than the system resources can handle. Two solutions are available to the congestion problem: either increase the resources or decrease the load.

A critical requirement of networks is the delivery of messages in a timely and predictable manner, and it is addressed with adequate network bandwidth and reliability. Bandwidth resources can be managed with quality of service management where resources are allocated and conflicts are resolved using the established security policies.

Quality of service (QoS) is a network performance property that specifies a guaranteed throughput level for end-to-end services, which is critical for most composite Web services in delivering enterprise-wide service-oriented distributed systems. Examples of network performance properties include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, and packet jitter.

Quality of protection (QoP) requires that overall performance of a system should be improved by prioritizing traffic and considering rate of failure or average latency at the lower layer protocols.

Denial of quality (DoQ) results from lack of quality assurance (QA) methods and QC techniques used in delivering messages, packets, and services. QA is the planned systematic activities necessary to ensure that a component, module, or system conforms to established technical requirements. QC is the prevention of defective components, modules, and systems. Proper implementation of QA methods and QC techniques can prevent DoQ and DoS and support QoS and QoP.

Denial of service (DoS) is the prevention of authorized access to resources or the delaying of time-critical operations.

Ways to improve QoS and QoP are listed next.

- Implement service-to-service authentication services as a part of authentication, authorization, and accountability concepts.
- Implement traffic prioritization rules to improve overall performance of the system.
- Implement Web service (WS)-Reliability and WS-Reliable Messaging standards for guaranteed message delivery and message ordering. These standards also address rate of failure or average latency at the lower layer protocols. Through WS-Reliable Messaging, Web services can ensure that messages are not lost even if the network is saturated.
- Use queuing networks and simulation techniques for both single service and composite services to ensure quality and availability of Web services. For example, enterprise systems with several business partners must complete business processes in a timely manner to meet real-time market conditions. The dynamic and compositional nature of Web services makes end-to-end QoS and QoP management a major challenge for service-oriented distributed systems.
- Ensure that packets corresponding to individual Web service messages are routed accordingly.
- Practice defensive programming techniques and the information hiding concept to make the Web service software more robust.
- Implement SLAs between an end-user organization and a service provider to satisfy specific end-user (customer) application system requirements.

6.4 Business Continuity

(a) Business Continuity Management

The entire scope of business continuity management (BCM) should be broader and more comprehensive than before. Its scope should be elevated to the enterprise level, similar to enterprise risk management, enterprise-wide resource planning software, enterprise customer relationship management system, enterprise-wide internal control systems, and enterprise-wide total quality management (TQM) programs. The reason for elevating BCM to the enterprise level is to integrate all the relevant pieces to determine the magnitude of disasters and incidents occurring in the entire enterprise in a timely manner for better and more complete action. The new BCM function should become a business-led initiative, not an IT–led initiative.

In the past, the BCM activities were focused more on IT function and less on business functions (e.g., operations, marketing, accounting, human resources [HR], and finance), leaving huge gaps and unmitigated risks to the overall enterprise.

The business-led processes should focus on these topics, for example:

- Addressing all business functions, including the IT function
- Handling IT continuity plans and disaster recovery plans (DRPs)
- Handling nature-made, man-made, and technology-used disasters
- Handling kidnapping of key executives and officers
- Understanding the applicable legal and regulatory requirements
- Ensuring that suppliers/vendors and business partners would continue to provide key raw materials, products, and services, even during disasters or incidents
- Handling cyber-based and terrorism-based attacks targeted at companies by hacking their computer systems and networks and stealing intellectual property information
- Implementing a vital records retention program
- Obtaining adequate insurance coverage for assets to recover losses

Implementing a vital records retention program and obtaining adequate insurance coverage is essential to ensuring BCM in order to protect assets from accidents, errors, disruptions, attacks, losses, damages, and disasters.

(i) Vital Record Retention Program

Vital records, whether maintained on paper or computer, should be retained according to internal requirements (e.g., management's policies and procedures on record keeping, record retention, storage, and disposal; and internal legal and audit requirements) and external requirements (e.g., legal, audit, regulatory, and tax guidelines). With respect to computer operations, record retention deals with retaining computer records, software, data files, directories, and libraries. Regarding electronic records, user organizations must ensure that the original software version that was used to create these records is still available and operable to retrieve the needed records. This requires policies and procedures to archive and test the original software and data quality.

(A) Retention of E-mail Messages E-mail messages should be treated the same way as paper documents that do the same things. E-mail is no more and no less important than other information used to transact business. All employees must apply the same decision-making process to e-mail that they apply to other documentary materials regardless of the media used to create them.

Records may not be retained in an e-mail directory. Any paper document can become an electronic record if issued via e-mail. Normally, only the originator copy is the record copy. Record documents may be retained in word processing directories or in hard-copy files, as long as they can be maintained in accordance with approved record schedules. Nonrecord material (e.g., transitory documents, copies, and drafts) may be retained in an e-mail directory for short periods. Delete all such material as soon as it has served its purpose.

E-mail directories should be purged routinely of material that is more than a certain period (e.g., 90 days) old. System administrators should accomplish this deletion after notice to system users that record material must be transferred from e-mail to appropriate scheduled files or directories.

(B) Retention of Tapes Tape management systems, which are used for data backup, have a vault management system that controls the movement of tape volumes from one storage location to another. Typically, critical tape volumes are cycled out of the central tape library to progressively more secure and less accessible storage areas, such as vaults, and then are finally transferred back to the central library. The retention of a vault tape can be based on one or more criteria, such as number of days elapsed since placed in vault, number of days since the tape was created, a specific hold time, or several others. Alternatively, an electronic vault can be used.

(C) Location of Electronic Records Because electronic records provide electronic evidence to a court of law as well as for fraud/crime investigators and law enforcement authorities, key challenges include whether these records will be available when needed or requested and how long they are available. Usually the data custodian of an organization decides how long to maintain them. Internet service providers (ISPs) retain records for a limited period, depending on what records are involved. For example, text messages may be retained for only a short time (e.g., two days). Another challenge is that electronic or paper records may often be stored in more than one place. Regarding e-mail messages, there could be multiple co-conspirators and multiple computers involved in a legal case, thus complicating the case analysis. Investigators need to search multiple locations to piece the key events together in order to issue simultaneous search warrants. It is even more challenging to deal with electronic records stored outside the country that were involved in trade secret and economic espionage cases. Efforts to obtain this electronic evidence from abroad can cause legal complications and delays.

(ii) Insurance Coverage

Implementing an effective insurance recovery program can complement the DRP. Insurance is a recovery control. Some organizations are self-insured and assume all risks while others take insurance coverage from insurance companies. Obtaining insurance coverage for computer-related property or equipment is no different from obtaining insurance for other types of property (e.g., building, machinery, and personal property). The insurance coverage should include software, hardware, and data. A complete property inventory is important not only for insurance purposes but also for disaster recovery planning. Four steps are involved in this process:

1. Determine the cost to replace each inventoried item.
2. Inquire where the item can be replaced.

3. Know the items that are irreplaceable.
4. Determine consequences if the items are lost.

There are at least three methods of property valuation: actual cash value, replacement value, and functional replacement value. Each is discussed next.

1. **Actual cash value** accounts for the replacement value of an item minus the actual depreciation and obsolescence that have lessened its value. The amount likely will not be enough to adequately replace what was lost.
2. **Replacement value** is the amount it costs to buy the exact piece of property, new, without deducting for depreciation. This is the most commonly used method of all.
3. **Functional replacement value** is the amount paid to replace obsolete machinery with up-to-date models. In rare cases, this cost actually may be less than the original value of the item being replaced.

(A) Coinsurance Requirements Once accurate values have been determined for all property items, the decision is the amount of insurance to carry. Usually, 80% coinsurance (insurance to value) is the standard, and it represents the percentage of recovery entitled in the event of a total loss. If less than 80% coinsurance is purchased, the cost of any loss sustained will be shared with the insurance company according to the percentage of coverage purchased.

(b) IT-Focused Continuity Management

Scope of contingency planning; scope of incident management; contingency planning strategies; scope of disaster recovery planning; develop recovery site strategies; develop alternate recovery site strategies; implementation, documentation, training, and testing; contingency plan maintenance, and fault-tolerance mechanisms are covered in this section.

(i) Scope of Contingency Planning

Computer-based application systems and business-related information systems must be available at all times to continue normal business operations and to handle and recover from disasters.

A **computer security contingency** is an event, incident, or disaster with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, software malfunction, fire, or storm. Disruptive events are of three types: man made, nature made, or technology used. Examples of man-made disruptions include vandalism, terrorism, economic espionage, sabotage, malicious mischief, arson, strikes, riots, and collisions from vehicles, trains, boats, and aircraft. Examples of nature-made disruptions include wind, rain, snow, sleet, lightning, flooding, tidal waves, moving ice, fire, earthquakes, and slides. Technology-used disruptions include cyberattacks and other attacks. To avert potential contingencies and disasters or to minimize the damage they cause, organizations can take steps early to control these events.

Generally called contingency planning, this activity is closely related to incident handling, which primarily addresses malicious technical threats, such as hackers and viruses. Other names given to contingency planning include disaster recovery, business continuity, continuity of operations, or business resumption planning. The contingency planning document and procedures must be useful in time of emergency. Computer hardware or software must have built-in fail-soft controls to provide continuity of operations.

Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization. Physical disaster prevention and preparedness begins when a data center site is first constructed. For example, the best location for a data center in a multistoried building is any floor other than the first floor, basement level, or top floor.

Disasters can happen without warning. The great losses that accrue as a result of a disaster are directly related to the side effects of the disaster, not the disaster itself. Management cannot prevent disasters; it can only detect, correct, or recover from them. DRPs and security policies are separate but complementary. The public relations department of an organization should act immediately after a disaster has occurred to notify the press and the public.

(A) Contingency Plan Undesirable events occur regardless of a security program's effectiveness. Contingency planning provides a controlled response that minimizes damage and restores operations as quickly as possible. A **contingency plan** is a document or set of documents that provides a course of action to be followed before, during, and after an undesirable event that disrupts or interrupts IT operations. The document should include procedures for data recovery, hardware recovery, and updating the contingency plan. The planning process should focus on providing a minimum acceptable level of outputs and services, using a combination of top-down and bottom-up approaches. It should also focus on a vital records program considering legal, tax, audit, regulatory, and business requirements.

A contingency plan should detail:

- Individual roles and responsibilities.
- Actions to be taken before an undesirable event occurs.
- Actions to be taken at the onset of an undesirable event to limit the level of damage, loss, or compromise of assets.
- Actions to be taken to restore critical IT functions.
- Actions to be taken to reestablish normal IT operations.

Contingency plans address both catastrophic events that cause major destruction to IT assets and less-than-catastrophic events that interrupt IT operations but do not cause major destruction. Contingency plans do not concentrate on disaster recovery planning to the detriment of planning for less-than-catastrophic occurrences. As a general rule, the greater the adverse impact of an undesirable event, the lower its probability of occurring. Contingency plans are stored onsite for use in less-than-catastrophic occurrences and offsite so that they will be available when needed.

To handle these undesirable events, organizations should do the following:

- Develop risk profiles.
- Establish security priorities.
- Identify critical applications.

(B) Business Impact Analysis The business impact analysis (BIA) is a critical step in implementing the contingency plan controls and in the contingency planning process overall. The BIA enables

management to characterize the system components, supported business functions, and their interdependencies. The BIA results characterize the consequences of a disruption, which is used to determine contingency planning requirements and priorities.

The BIA should critically:

1. Examine the business processes and their dependencies.
2. Assess costs and benefits.
3. Locate single points of failure.
4. Identify risks and threats (both physical and environmental).

For example, a single point of failure occurs when there is no redundancy in data, equipment, facilities, systems, and programs. Risks in the use of cellular radio and telephone networks during a disaster include security systems and switching offices.

The BIA should be performed during the initiation phase of the SDLC using both quantitative and qualitative tools. Three steps typically are involved in accomplishing the BIA:

1. **Determine mission or business functions and recovery criticality.** Business functions supported by the system are identified and the impact of a system disruption to those functions is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the business functions.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources needed to resume business functions and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, supplies, and vital records.
3. **Identify recovery priorities for system resources.** Based on the results from the previous activities, system resources can be linked more clearly to critical business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

(C) Identify and Prioritize Critical Business Functions When developing an IT contingency plan, the first step is to establish a contingency planning policy within the organization. This policy may exist at the department, division, and/or program level of the organization. The statement should do three things:

1. Define the organization's overall contingency objectives.
2. Identify leadership roles and responsibilities; resource requirements; and test, training, and exercise schedules.
3. Develop maintenance schedules and determine the minimum required backup frequency.

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. The definition of an organization's critical mission or business function is often called a business plan.

Since the business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses but also to set priorities for them. A fully redundant capability for each function is prohibitively expensive for most organizations. In the event of a disaster, certain functions will not be performed based on careful decisions. If appropriate priorities have been set and approved by senior management, it could mean the difference in the organization's ability to survive a disaster.

After identifying critical missions and business functions, it is necessary to identify the supporting resources, the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how resources interact to support the organization's mission or business. Many of these resources are not computer resources. Contingency planning should address all the resources needed to perform a function, regardless of whether they directly relate to a computer.

The analysis of needed resources should be controlled by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organization to assign priorities to resources since not all elements of all resources are crucial to the critical functions. *In many cases, the longer an organization is without a resource, the more critical the situation becomes.*

(D) Maximum Tolerable Downtime Maximum tolerable downtime (MTD) represents the total amount of time the system owner is willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content. MTD is also known as maximum allowable outage (MAO), which describes the downtime threshold. MTD and recovery time objective (RTO) replace MAO.

Additional processing time (APT) is required when a system outage may prevent a particular process from being completed. Because it takes time to reprocess the data, that APT must be added to the RTO to stay within the time limit established by the MTD.

(E) Assess Exposure to Outages (Local, Regional, National, or Global) Although it is impossible to think of all the things that can go wrong (i.e., outages), the next step is to identify a likely range of problems. The development of **scenarios** will help an organization develop a plan to address the wide range of things that can go wrong. Scenarios should include small and large contingencies and best case, worst case, and most likely cases. Creating them requires imagination and creativity.

(F) Recovery Objectives Two types of recovery objectives exist: RTO and recovery point objective (RPO).

RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business functions, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and when the MTD is inflexible, a plan of action and milestone should be initiated to document the situation and plan for its mitigation.

RTOs for essential business functions must be sustained within 12 hours and for up to 30 days from an alternate site, what are determined by the system-based BIA. Nonessential business functions do not require an alternate site as part of the recovery strategy but may require security controls similar to an alternate site.

The contingency plan coordinator, working with management, should determine the optimum point to recover the information system by addressing the factors mentioned earlier while balancing the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical business functions.

The longer a disruption is allowed to continue, the more costly it can become to the organization and its operations. Conversely, the shorter the RTO, the more expensive the recovery solutions cost to implement. For example, if the system must be recovered immediately for a high-impact system, zero downtime solutions and alternate processing site costs will be much higher. A low-impact system with a longer RTO would be able to implement a less costly simple tape backup system. Plotting a graph between the cost and the length of disruption time will show an optimal point called the cost balance point, where the cost to recover line intersects with the cost of disruption line (business downtime). The cost balance point will be different for every organization and system based on financial constraints and operating requirements. Note that the cost to recover a mirrored system is high and the cost to recover a tape backup system is low.

WHAT IS RECOVERY POINT OBJECTIVE, RECOVERY TIME OBJECTIVE, AND MAXIMUM TOLERABLE DOWNTIME, AND HOW ARE THEY RELATED TO BUSINESS IMPACT ANALYSIS?

- An RPO is the point in time in which data must be restored in order to resume computer processing.
- An RTO is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.
- An MTD is the total amount of time the system owner is willing to accept for a business process outage or disruption and includes all impact considerations.
- Note that the BIA must consider the RPO, RTO, and MTD since they are related to and affect each other.
- Note that RPO and RTO are a part of disaster recovery controls and procedures.

The RPO represents the point in time, prior to a disruption or system outage, to which business process data can be recovered (given the most recent backup copy of the data) after an outage. Because the RTO must ensure that the MTD is not exceeded, the RTO normally must be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that APT must be added to the RTO to stay within the time limit established by the MTD. These relationships are shown next.

$$\text{BIA} \rightarrow \text{MTD, RTO, and RPO}$$
$$\text{RTO} < \text{MTD}$$
$$\text{RTO} + \text{APT} < \text{MTD}$$

(ii) Scope of Incident Management

(A) Security Incident Triad The security incident triad includes three elements: detect, respond, and recover. An organization should have the ability to detect an attack, respond to an attack, and recover from an attack by limiting consequences of or impacts from an attack.

The security incident triad is the emergency response capability for various technical threats, such as hackers and viruses. Incident handling can also help an organization prevent future incidents. These questions should be raised:

- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents (i.e., what files and logs should be kept, whom to contact, and when)?
- Who receives and responds to alerts or advisories (e.g., vendor patches or exploited vulnerabilities)?
- What preventive measures are in place (i.e., intrusion detection tools, automated audit logs, or penetration testing)?

Root cause analysis can be used in the remediation step of the incident response. Root cause analysis is a problem-solving tool, using a cause-and-effect (C&E) diagram. This diagram is used for analyzing when a series of events or steps in a process creates a problem and it is not clear which event or step is the major cause of the problems. After examination, significant root causes of the problem are discovered, verified, and corrected. The C&E diagram is also called a fishbone or Ishikawa diagram and is a good application in managing a computer security incident response as a remediation step.

(B) Symptoms of an Incident It is always possible that a computer system or network may be compromised by an intentional or unintentional incident. When several symptoms start to appear, a pattern may indicate that a system is under attack, and the situation may be worth investigating further. If the adversary is skilled, it may not be very obvious that an attack is under way. The symptoms of an incident could include any of the following:

- Unusually heavy network traffic
- Out-of-disk space alert or significantly reduced free disk space
- Unusually high central processing unit (CPU) usage
- Creation of new user accounts and accounts in use when the user is not at work
- Attempted or actual use of administrator-level accounts and locked-out accounts
- Cleared log files and full log files with unusually large number of events
- Antivirus alerts or alerts from the intrusion detection system and disabled antivirus software
- Unexpected patch changes and unexpected changes in configuration settings
- Computers and communication devices connecting to outside Internet Protocol (IP) addresses
- Requests for information about a system-related data such as user identifications (IDs) and passwords (i.e., social engineering attempts)
- Unexpected system shutdown or slowdown

INCIDENT HANDLING VERSUS CONTINGENCY PLANNING

An incident-handling capability may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

(C) Benefits Two types of benefits are accrued from incident management: primary and secondary (side benefits). The primary benefits are containing and repairing damage from incidents and preventing future damage. The side benefits include use of threat and vulnerability of data, enhancing internal communications and organization preparedness, and enhancing the training and awareness program.

(D) Help Desk The help desk function should be closely linked to an organization's incident response handling capability because in many cases the same staff members perform these two functions.

(iii) Contingency Planning Strategies

Procedures for executing the recovery strategy should be outlined in the contingency plan. The plan must be written in a format that will provide the users (recovery team leadership and members) the context in which the plan is to be implemented and the direct procedures, based on role, to execute. The plan includes notification and activation procedures, damage assessment, sequence of recovery activities, restore original site, testing systems, and terminating operations.

The next thing is to plan how to recover needed resources. It is a fact that there is no recovery without a backup. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimize contingencies. Since no set of controls can cost effectively prevent all contingencies, it is necessary to coordinate prevention and recovery efforts.

A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption (restoration). **Emergency response** encompasses the initial actions taken to protect lives, limit property damage, and minimize the impact of the emergency. Contingency planning for local area networks (LANs) should consider security incident response, backup operations, and recovery plans. **Recovery** refers to the steps taken to continue support for critical functions. A proactive DRP includes a UPS, an emergency procedure, and a fire extinguisher. **Resumption** is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

The selection of a strategy needs to be based on practical considerations, including feasibility and cost. The different categories of resources should be considered separately. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a power generator or to move computer processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Are the consequences of a loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is unclear which strategy is best.

An incident-handling capability plan might call for at least one manager and one or more technical staff members to accomplish program objectives. Depending on the scope of the effort, however,

full-time staff members may not be required. In some situations, some staff may be needed part time or on an on-call basis. Personnel may be performing incident-handling duties as an adjunct responsibility to their normal assignments.

A training and awareness program can benefit from lessons learned during incident handling. Incident-handling staff will be able to help assess the level of user awareness about current threats and vulnerabilities. Staff members may be able to help train system administrators, system operators, and other users and systems personnel. Knowledge of security precautions (resulting from such training) helps reduce future incidents. It is also important that users are trained what to report and how to report it.

Incident-handling staff will need to keep current with computer system and security developments. Budget allowances need to be made, therefore, for attending conferences, security seminars, and other continuing education events. If an organization is located in more than one geographic area, funds probably will be needed for travel to other sites for handling incidents.

(iv) Scope of Disaster Recovery Planning

A DRP is essential to continued availability of computer systems. The DRP should include the following items:

- Required response to events or conditions of varying duration and severity that would activate the recovery plan
- Procedures for operating the computer system in manual mode without external electronic connections
- Roles and responsibilities of responders (first and second responders)
- Processes and procedures for the backup and secure storage of information
- Complete and up-to-date logical network diagrams
- Personnel list for authorized physical and cyber-access to computer systems
- Communication procedures and list of personnel to contact in the case of an emergency including vendors, network administrators, and support staff (call tree list)
- Current configuration information for all components of systems
- Replacement for hard-to-obtain critical components kept in inventory

The DRP plan should define a comprehensive backup and restore policy. In formulating this policy, these issues should be considered:

- The speed at which data or the system must be restored. This requirement may justify the need for a redundant system, spare offline computer, or valid file-level system backups.
- The frequency at which critical data and configurations are changing. This will dictate the frequency and completeness of backups.
- The safe onsite and offsite storage of full and incremental backups.
- The safe storage of installation media, license keys, and configuration information.
- Identification of individuals responsible for performing, testing, storing, and restoring backups.

(v) Develop Recovery Site Strategies

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and MAO times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. Specific recovery methods should be considered and may include these types:

- Commercial contracts with cold, warm, or hot site vendors
- Mobile sites
- Mirrored sites
- Reciprocal agreements with internal or external organizations
- SLAs with equipment vendors

In addition, technologies such as RAID, automatic fail-over, UPS, and mirrored systems should be considered when developing a system recovery strategy.

When a disruption occurs despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the RTO period. The recovery strategy is designed from a combination of methods that together address the full spectrum of information system risks. Several options may be evaluated during the development phase; the most cost effective, based on potential impact, should be selected and integrated into the information system architecture and operating procedures.

The contingency planning coordinator should determine the optimum point to recover the IT system by balancing the cost of system inoperability against the cost of resources required for restoring the system. This is called **recovery cost balancing**. Where the cost of disruption line and the cost to recover line (on a cost versus time graph) meet defines how long the organization can afford to allow the system to be disrupted or unavailable.

Systems and data must be backed up regularly; therefore, all IT contingency plans should include a method and frequency for conducting data backups. The frequency of backup methods—daily or weekly, incremental, differential, or full—should be selected based on system criticality when new information is introduced. The backup method selected should be based on system and data availability and integrity requirements (as defined in the BIA). Data that are backed up may need to be stored offsite and rotated frequently, depending on the criticality of the system. A backup-in-depth strategy is better than a single-level backup strategy.

Major disruptions to system operations may require **restoration activities** to be implemented at an alternate site. The type of alternate site selected must be based on RTO requirements and budget limitations. Equipment for recovering and/or replacing the information system must be

provided as part of the recovery strategy. Cost, delivery time, and compatibility factors must also be considered when determining how to provide the necessary equipment. Organizations must also plan for an alternate site that, at a minimum, provides workspace for all contingency plan personnel, equipment, and the appropriate IT infrastructure necessary to execute IT contingency plan and system recovery activities. The level of operational readiness of the alternate site is an important characteristic to determine when developing the recovery strategy.

(A) Offsite Storage Offsite storage locations should be identified to store magnetic media, paper documentation, and forms needed to run the backup computer in the event of a disaster. Care should be taken to select an offsite storage location, whether it is a part of the organization or an outside commercial storage center situated locally or remotely to the primary computer center. Regardless of the choice, the offsite storage location should be well controlled in terms of record keeping of movement of media and documentation between onsite and offsite, adequate physical security over the facilities, and environmental controls within the facility.

It is good business practice to store backed-up data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data are backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data are required for recovery or testing purposes, the organization contacts the storage facility requesting transport of specific data to the organization or to an alternate facility. Backup tapes should be tested regularly to ensure that data are being stored correctly and that the files may be retrieved without errors or lost data. Also, the contingency planning coordinator should test the backup tapes at the alternate site, if applicable, to ensure that the site supports the same backup configuration that the organization has implemented. Commercial storage facilities often offer media transportation and response and recovery services.

Full-volume backups and incremental backups are two common methods used to back up system/file contents. In full-volume backups, the entire disk volume is backed up regardless of the changes made to individual files in a volume. In incremental backups, only changes since the last backup are backed up, which saves time. Storing backup files and documentation offsite is the best corrective control.

The backup files should include current and critical master files, transaction files, OS application source programs, and compiled object programs. Other documentation should include system-related documentation, the phone contact list, and a supply of special forms.

The type of data to be stored offsite depends on legal, business, and regulatory requirements. The frequency of backup depends on whether it is an online or a database system. For example, online systems require a periodic dump of transaction logs, and the database is backed up hourly. To restore a file, the previous day's backup file and the current transaction file are needed. Inadequate documentation, lack of audit trails, inability to resolve system deadlocks, or lack of passwords could delay system recovery at an offsite backup facility.

When selecting an offsite storage facility and vendor, these criteria should be considered:

- **Geographic area.** Distance from the organization and the probability of the storage site being affected by the same disaster as the organization
- **Accessibility.** Length of time necessary to retrieve the data from storage and the storage facility's operating hours

- **Security.** Security capabilities of the storage facility and employee confidentiality, which must meet the data's sensitivity and security requirements
- **Environment.** Structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)
- **Cost.** Cost of shipping, operational fees, and disaster response/recovery services

(B) Tape Rotation Usually tape files are backed up using a three-generation (son, father, and grandfather) concept, where each generation represents a time period (e.g., seven or five operating days). Disk files are saved for five or seven generations. Each generation can have multiple copies and be rotated between onsite and offsite. Tape files are a major obstacle to unattended computer center operation due to their labor-intensive nature.

(C) Electronic Vaulting The manual mode of performing system backups is time consuming, labor intensive, and costly because physical tape vaulting and tape rotation are required. **Electronic vaulting** is the ability to store and retrieve backups electronically, in a site remote from the primary computer center. The backup information can be transmitted to offsite from onsite and vice versa. Optical disk, magnetic disk, mass storage device, and the automated tape library are some examples of storage media devices used on the receiving end of an electronic vault. Electronic vaulting exploits the significant cost/performance improvements made in telecommunications technologies. The higher bandwidth and lower costs associated with fiber optics and satellite links have made it possible to send complete backup image copies electronically. It is also possible to vault current transaction recovery information (log or journal data) to the remote site in a timely manner.

The **benefits** of electronic vaulting are: improved system availability, system performance, and system reliability; quality of the backup and recovery processes; and increased customer (user) service and satisfaction. Electronic vaulting makes backup information more accessible by reducing the retrieval time from hours or days to minutes during an interruption or a disaster when time is most valuable. Depending on the application, less information can be maintained online in the computer center, which in turn reduces the amount of onsite backup storage needed. This method supports automated or unattended computer center operations because minimal or no human intervention is required.

An electronic vault can be located in these areas:

- At a primary recovery site
- At an alternate recovery site
- At a reciprocal site (i.e., recovery at the development site and production on the other site)
- In a third-party location close to the primary recovery site
- At a commercial hot/cold site facility

(vi) Develop Alternate Recovery Site Strategies

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, for all high-impact and moderate-impact systems, the plan should include a strategy to recover and perform system operations at an alternate site/facility for an extended period. Organizations may consider low-impact systems for alternate site processing, but such site is not required due to their low risk and is dependent on management's decision.

- High-impact systems require mirrored systems with disk replication; high-availability systems; and a hot site, mobile site, or mirrored site, or a combination of these sites
- Medium-impact systems require a warm site
- Low-impact systems require a cold site or a reciprocal agreement

In general, three types of alternate sites are available:

1. Dedicated site owned or operated by the organization (i.e., company owned or operated, which is very expensive).
2. Reciprocal agreement requiring a memorandum of agreement (MOA) or a memorandum of understanding (MOU) with an internal or external entity. Internal entities may require an MOU while external entities may require an MOA.
3. Commercially leased facility (e.g., cold site, warm site, or hot site).

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, and hot sites, progressing from basic to advanced, as follows:

Cold Site → Warm Site → Hot Site

Other variations of the three common sites include mobile sites and mirrored sites with similar core features. A brief discussion of cold sites, warm sites, hot sites, mobile sites, mirrored sites, reciprocal agreements, SLAs, and hybrid approaches.

(A) Cold Sites Cold sites are locations that have the basic infrastructure and environmental controls available (e.g., electrical, heating, and air conditioning), but no equipment or telecommunications established or in place. There is sufficient room to house needed equipment to sustain a system's critical functions. Examples of cold sites include unused areas of a data center and unused office space (if specialized data center environments are not required). Cold sites are normally the least expensive alternate processing site solution, as the primary costs are only the lease or maintenance of the required square footage for recovery purposes. However, the recovery time is the longest, as all system equipment (including telecommunications) will need to be acquired or purchased, installed, tested, and have backup software and data loaded and tested before the system can be operational. Depending on the size and complexity of a system, recovery could take several days to weeks to complete. The cold site method is most difficult and expensive to test compared to the hot or warm site method.

(B) Warm Sites Warm sites are locations that have the basic infrastructure of cold sites but also have sufficient computer and telecommunications equipment installed and available to operate the system at the site. However, the equipment is not loaded with the software or data required to operate the system. Warm sites should have backup media readers that are compatible with the system's backup strategy. Warm sites may not have equipment to run all systems or all components of a system, just enough to operate critical mission/business functions. An example of a warm site is a test or development site that is geographically separate from the production system. Equipment may be in place to operate the system but would require reverting to the current production level of the software, loading the data from backup media, and establishing communications to users. Another example is available equipment at an

alternate facility that is running noncritical systems and that could be transitioned to run a critical system during a contingency event. A warm site is more expensive than a cold site, as equipment is purchased and maintained at the site, with telecommunications in place. Some costs may be offset by using equipment for noncritical functions or for testing. Recovery to a warm site can take several hours to several days, depending on system complexity and the amount of data to be restored.

(C) Hot Sites Hot sites are locations with fully operational equipment and capacity to quickly take over system operations after loss of the primary system facility. A hot site has sufficient equipment and the most current version of production software installed, and adequate storage for the production system data. Hot sites should have the most recent version of backed-up data loaded, requiring only updating with data since the last backup. In many cases, hot site data and databases are updated concurrently with or soon after the primary data and databases are updated. Hot sites also need a way to quickly move system users' connectivity from the primary site. One example of a hot site is two identical systems at alternate locations that are in production, serving different geographical locations or load-balancing production workloads. Each location is built to handle the full workload, and data are continuously synchronized between the systems. This is the most expensive option, requiring full operation of a system at an alternate location and all telecommunications capacity, with the ability to maintain or quickly update the operational data and databases. Hot sites also require having operational support nearly equal to the production location. Recovery to a hot site can take minutes to hours, depending on the time needed to move user connectivity to the new location and make data current at the hot site location. A hot site is used for short-term needs while a cold site is used for long-term needs.

(D) Mobile Sites Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

(E) Mirrored Sites Mirrored sites are fully redundant facilities with automated real-time information mirroring. A mirrored site (redundant site) is equipped and configured exactly like the primary site in all technical respects. Some organizations plan on having partial redundancy for disaster recovery purposes and partial processing for normal operations. The stocking of spare personal computers (PCs) and their parts or LAN servers also provide some redundancy. Exhibit 6.17 summarizes the five alternate sites

Alternate Site	Cost	Hardware/ Equipment	Telecommunications	Setup time	Location
Cold site	Low	None	None	Long	Fixed
Warm site	Medium	Partial	Partial/full	Medium	Fixed
Hot site	Medium/high	Full	Full	Short	Fixed
Mobile site	High	Dependent	Dependent	Dependent	Not fixed
Mirrored site	High	Full	Full	None	Fixed

EXHIBIT 6.17 Five Alternative Sites

(F) Reciprocal Agreements Reciprocal agreements occur when two or more organizations with similar or identical system configurations and backup technologies enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement with an MOA or MOU. A reciprocal agreement should be entered into carefully because each site must be able to support the other, in addition to its own workload, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy. Consideration should also be given to system interconnections and possible interconnection security agreements.

(G) Service-Level Agreements for Alternate Recovery Sites An MOA/MOU or an SLA for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department and audit department of each party must review and approve the agreement. In general, the SLA should address at a minimum, each of these elements:

- Contract/agreement duration
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures)
- Site/facility priority access and/or use
- Site availability
- Site guarantee
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable
- Contract/agreement change or modification process
- Contract/agreement termination conditions
- Process to negotiate extension of service
- Guarantee of compatibility
- Information system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software)
- Change management and notification requirements, including hardware, software, and infrastructure
- Security requirements, including special security needs
- Staff support provided/not provided
- Facility services provided/not provided (e.g., use of onsite office equipment and cafeteria)
- Testing, including scheduling, availability, test time duration, and additional testing, if required

- Records management (onsite and offsite), including electronic media and hard copy
- Service-level management (performance measures and management of quality of information system services provided)
- Workspace requirements (e.g., chairs, desks, telephones, and PCs)
- Supplies provided/not provided (e.g., office supplies)
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

(H) Hybrid Approaches to Alternate Sites Some organizations use any combination of the preceding approaches in what is called a hybrid approach. It includes having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

(vii) Implementation, Documentation, Training, and Testing

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations for implementation, document the strategies, train employees, and test. Many of these tasks are ongoing.

(A) Implementation Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly, and so should backup services and redundant equipment. Contracts and agreements also may need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people often are referred to as the contingency response team. This team often is composed of people who were a part of the contingency planning team.

There are many important implementation issues for an organization. Two of the most important are: How many plans should be developed? and Who prepares each plan? Both of these questions revolve around the organization's overall strategy for contingency planning. The answers should be documented in an organization's policy and procedures manual.

(B) Documentation The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge can immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any offsite locations, such as alternate processing sites or backup data storage facilities.

(C) Training All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills.

Training is particularly important for effective employee response during emergencies. If there is a fire, there is no time to check a manual to determine correct procedures. Depending on the nature of the emergency, there may or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

(D) Testing A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specially assigned. The extent and frequency of testing will vary between organizations and among systems. Regardless, recovery strategy should be revised based on the test results and lessons learned. *There are several types of testing, including reviews, analyses, disaster simulations, end-to-end testing, and full-scale testing as discussed later in this chapter.*

Reviews A review can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures. *A checklist is used during reviews to ensure that all items are addressed.*

Analyses An analysis, or desk checking, may be performed on the entire plan or portions of it, such as emergency response procedures. It is beneficial if the analysis is performed by someone who did not help develop the contingency plan but has a good working knowledge of the critical function and supporting resources. The analyst(s) may mentally follow the strategies in the contingency plan, looking for flaws in the logic or processes used by the plan's developers. The analyst also may interview functional managers, resource managers, and their staff to uncover missing or unworkable pieces of the plan.

Disaster Simulations Organizations may also arrange disaster simulations. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost beneficial it is to perform a disaster simulation.

End-to-End Testing The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, interoperate as intended in an operational environment (either actual or simulated). These interrelated systems include not only those owned and managed by the organization but also the external systems with which they interface.

Generally, end-to-end testing is conducted when one major system in the end-to-end chain is modified or replaced, and attention is rightfully focused on the changed or new system. The boundaries on end-to-end tests are not fixed or predetermined but vary depending on a given business area's system dependencies (internal and external) and criticality to the mission of the organization. Therefore, in planning end-to-end tests, it is critical to analyze the organization's

core business functions, the interrelationships among systems supporting these functions, and potential risk exposure due to system failures in the chain of support. It is also important to work early and continuously with the organization's data exchange partners so that end-to-end tests can be effectively planned and executed.

Full-Scale Testing Full-scale (full-interruption) testing is costly and disruptive while end-to-end testing is least costly and less disruptive. Management of a firm will not allow stopping of normal production operations for the sake of full-interruption testing. Some businesses operate on a 24/7 schedule, and losing several hours or days of production time is equal to another disaster, financial or otherwise. Hence, full-scale testing is not advised unless overruled by management.

The contents of personnel **training program** document should include the following:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (i.e., activation/notification, recovery, and reconstitution phases)
- Individual responsibilities (i.e., activation/notification, recovery, and reconstitution phases)

The contents of a **testing program** document should include the following:

- System recovery on an alternate site from backup media
- System performance using alternate equipment
- Coordination among recovery teams (e.g., business continuity planners)
- Restoration of normal operations
- Internal and external connectivity
- Notification procedures

The contents of an **exercise program** document should include the following:

- Tabletop exercises (i.e., discussion based only without the deployment of equipment is useful for low-impact systems)
- Functional exercises (i.e., validation of operational readiness for emergencies is useful for moderate-impact systems with system recovery from backup media)
- Full-scale functional exercises (i.e., a system failover to the alternate site, recovery of a server or database from backup media, and processing from a server at an alternate site are useful for high-impact systems with full system recovery and reconstitution to a known state)
- Personnel exercises (i.e., execution of staff roles and responsibilities)
- Scenario-driven exercises (i.e., simulation of operational emergency environment such as a power failure or a fire in a data center).

Functional, full-scale functional, and personnel exercises are examples of scenario-driven exercises.

(viii) Contingency Plan Maintenance

The IT contingency plan must always be maintained in a ready state for use immediately upon notification. Periodic reviews of the plan must be conducted for currency of key personnel and vendor information, system components and dependencies, the recovery strategy, vital records, and operational requirements. While some changes may be obvious (e.g., personnel turnover or vendor changes), others will require analysis. The business impact analysis (BIA) should be reviewed periodically and updated with new information to identify new contingency requirements and priorities. Changes made to the plan are noted in a record of changes, dated, and signed or initialed by the person making the change. The revised plan (or plan sections) is circulated to those with plan responsibilities. Because of the impact that plan changes may have on interdependent business processes or information systems, the changes must be clearly communicated and properly annotated in the beginning of the document.

(A) Fault-Tolerance Mechanisms Maintenance Modern fault-tolerance mechanisms can play an important role in maintaining data and system integrity as they increase system resilience. Resilience is the ability of a computer system to continue to perform its tasks after the occurrence of faults and to operate correctly even though one or more of its component parts are malfunctioning. Traditional system fault-tolerance mechanisms, such as logs and locks, cannot handle serious malicious code attacks or cyberattacks. The ultimate goal is to ensure that computer systems are reliable and available for system users.

Some examples of fault-tolerance mechanisms are listed next.

- Develop error detection, error correction, and redundant processing policies and procedures to maintain integrity of data and systems.
- Install mechanisms such as fail-stop processors and redundancy mechanisms with built-in fault detection, error recovery, and failure recovery abilities combined with system reliability measurement metrics (e.g., mean time to failure [MTTF], mean time to repair [MTTR], and mean time between failures [MTBF]).
- Install fault-tolerant hardware methods, as they increase system resilience.
- Install a robust OS so it can handle unexpected system failures.

System Redundancy Mechanisms Some concepts regarding system redundancy mechanisms are listed next.

- Increasing system redundancy will increase system reliability, availability, and serviceability.
- The need for redundant electrical power is often overlooked during contingency plan development.
- Network availability is increased with redundancy in electrical power.
- Meshed network topology provides a high degree of fault tolerance when compared to star, bus, and ring topologies.
- Network reliability is increased with alternate telecommunications carriers.
- Normal Ethernet does not have built-in redundancy. Fast Ethernet, Fiber Distributed Data Interface (FDDI), and Synchronous Optical Network (SONET) have built-in redundancy or have options for it.

- Implement disk mirroring, disk shadowing, server mirroring, disk duplexing, block mirroring, check-pointing, disk farming, and disk arrays concepts to reduce or eliminate downtime from disk failure or loss of data.

System Reliability Measurement Metrics Some examples of system reliability measurement metrics are listed next.

- MTTF is the average time to the next failure. It is the time taken for a part or system to fail for the first time. MTTF assumes that the failed system is not repaired. A high MTTF means high system reliability.
- MTTR is the amount of time it takes to resume normal operation. It is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time. A low MTTR means high system reliability.
- MTBF is the average length of time a system is functional or the average time interval between failures. It is total functioning life of an item divided by the total number of failures during the measurement interval of minutes, hours, and days. It is the average length of time a system or a component works without fault between consecutive failures. MTBF assumes that the failed system is immediately repaired, as in MTTR (repair). A high MTBF means high system reliability.

$$\text{MTBF} = \text{MTTF} + \text{MTTR (repair)}$$

SYSTEM RELIABILITY VERSUS SYSTEM AVAILABILITY

- The reliability of a computer system is defined as the probability that the system will be able to process work correctly and completely without its being terminated or corrupted.
- The availability of a computer system is a measure of the amount of time that the system is actually capable of accepting and performing a user's work.
- System reliability can be thought of as the quality of service. System availability can be thought of as the quantity of service. In other words, availability can be considered a component of reliability.
- A system that fails frequently but is restarted quickly has high availability even though its reliability is low.
- System reliability is related to system safety and quality, not system availability.
- Note that the terms "reliability" and "availability" are closely related but are often incorrectly used as synonyms.

- MTTR is the time following a failure to restore a RAID disk array to its normal failure-tolerant mode of operation. This time includes replacement of the failed disk and the time to rebuild the disk array. A low MTTR means high system availability.
- Mean time between outages (MTBO) is the mean time between equipment failures that result in a loss of system continuity or unacceptable degradation, as expressed by:

$$\text{MTBO} = \text{MTBF}/(1-\text{FFAS})$$

where
MTBF = Nonredundant mean time between failures
FFAS = Fraction of failures for which the failed hardware or software is bypassed automatically

A low MTBO means high system availability.

- MTTR is the average time to restore service following system failures that result in service outages. The time to restore includes all time from the occurrence of the failure until the restoral of service. A low MTTR means high system availability.
- Mean time to data loss (MTTDL) is the average time before a loss of data occurs in a given disk array and is applicable to RAID technology. A low MTTDL means high data reliability.
- Time to recover (TTR) is the time required for any computer resources to be recovered from disruptive events. It is the time required to reestablish an activity from an emergency or degraded mode to a normal mode. Note that TTR is also defined as emergency response time (EMRT).

Fault-Tolerance Hardware Methods These methods should be implemented in combination to improve the performance of data storage media regardless of the type of computer used:

- Disk arrays
- Disk striping
- Disk mirroring
- Server mirroring
- Disk duplexing
- Block mirroring
- Disk replication
- Disk imaging
- Disk farming
- Check-pointing

These methods are examples of fault-tolerant hardware methods. A gap between CPU and data storage subsystem performance causes imbalance, which in turn degrades online system response time and batch job turnaround time.

Disk arrays use a parity disk scheme to keep track of data stored in a domain of the storage subsystem and to regenerate it in case of hardware/software failure. A disk array unit contains many ready-to-use and standby disks. When one disk in the array fails, a spare disk automatically fills in and operates. Data are rebuilt from the parity disk. Disk arrays consume less overhead than disk mirroring and hence can be thought of as an alternative to disk mirroring. Disk arrays can be used to improve data transmission rates by improving input and output rates. They can fill the performance gap between the CPU and the storage subsystem. RAID has seven categories from 0 through 6, RAID-0 provides lower performance and RAID-6 provides higher performance characteristics when used with larger number of physical disks (i.e., 10 to 20). RAID technology increases fault tolerance of hardware and uses several disks in a single logical subsystem. The main purpose of RAID is to provide backup so if one disk fails, all of the data are immediately available from the other disks. RAID storage units offer fault-tolerant hardware. The purpose of disk arrays is same as the disk striping, disk mirroring, and server mirroring.

Disk striping uses more than one disk and more than one partition, and is the same as disk arrays. An advantage of disk arrays include running multiple drives in parallel, and a disadvantage

includes the fact that its organization is more complicated than disk farming and highly sensitive to multiple failures.

Disk mirroring means that the file server contains duplicate disks, and all information is written to both disks simultaneously. It is same as disk shadowing.

Server mirroring means that the server is duplicated instead of the disk, which is expensive. All information is written to both servers simultaneously. Server mirroring serves the same purpose as disk arrays do.

Disk duplexing means that the disk controller is duplicated. When one disk controller fails, the other one is ready to operate.

Block mirroring is a method to provide backup, redundancy, and failover processes to ensure high availability of systems. Block mirroring is performed on an alternate site, preferably separate from the primary site. Whenever a data write is made to a block on a primary storage device at the primary site, the same write is made to an alternate storage device at the alternate site, either within the same storage system or between separate storage systems, at different locations.

In **disk replication**, data are written to two different disks to ensure that two valid copies of the data are always available. Disk replication minimizes the time windows for recovery.

Disk imaging is generating a bit-for-bit copy of the original media, including free space and slack space. Disk imaging is used in forensics evidence.

In **disk farming**, data are stored on multiple disks for reliability and performance reasons.

Check-pointing is a fault-recovery and restore procedure that is needed before, during, or after completion of certain transactions or events to ensure acceptable fault recovery.

(B) Robust Operating Systems An OS must be robust enough to withstand system failures. The OS response to failures can be classified into three general categories: system reboot, emergency system restart, and system cold start.

System reboot is performed after shutting down the system in a controlled manner in response to a trusted computing base (TCB) failure. For example, when the TCB detects the exhaustion of space in some of its critical tables or finds inconsistent object data structures, it closes all objects, aborts all active user processes, and restarts with no user process in execution. Before restart, however, the recovery mechanisms make a best effort to correct the source of inconsistency. Occasionally the mere termination of all processes frees up some important resources, allowing restart with enough resources available. Note that system rebooting is useful when the recovery mechanisms can determine that TCB and user data structures affecting system security and integrity are, in fact, in a consistent state.

Emergency system restart is done after a system fails in an uncontrolled manner in response to a TCB or media failure. In such cases, TCB and user objects on nonvolatile storage belonging to processes active at the time of TCB or media failure may be left in an inconsistent state. The system enters maintenance mode, recovery is performed automatically, and the system restarts with no user processes in progress after bringing up the system in a consistent state.

System cold start takes place when unexpected TCB or media failure takes place and the recovery procedures cannot bring the system to a consistent state. TCB and user objects may remain in an inconsistent state following attempts to recover automatically. Intervention of administrative personnel is now required to bring the system to a consistent state from maintenance mode.

(c) Roles and Responsibilities of Business Continuity Manager or Executive

Because each organization' size and scope are different, the roles and responsibilities of a business continuity manager or executive are different too. Because this position is diversified and unique, it should serve in more of a liaison role with coordination and cooperation from several functions within the organization. Regarding reporting relationships, the business continuity manager or executive should functionally report to the chief executive officer (CEO) and administratively report to the chief information officer (CIO) for independence and objectivity reasons. This reporting relationship is similar to cases when CIO reports to the CFO instead of the CEO and when the chief audit executive (CAE) reports to the CFO instead of functionally reporting to the board of directors and administratively to the CEO.

Specific roles and responsibilities of a business continuity manager or executive are listed next.

- Develop policies and procedures in handling normal (regular) and emergency disasters and incidents.
- Coordinate with business functional managers (e.g., accounting, finance, operations, and marketing), insurance manager, physical security officer, information security manager, and risk manager.
- Work with the insurance department to understand various insurance policy types, coverage, and limits, for equipment, buildings, and machinery. Also, understand the reinsurance provisions and limits.
- Work with the record-keeping department to ensure that both manual records and electronic records are properly retained, labeled, preserved, and stored in a safe and secure place. Ensure that the electronic records can be retrieved at a later date, so the corresponding software must be retained. Be familiar with the International Organization for Standardization (ISO) standard issued on record keeping (ISO 15489).
- Regularly meet with various stakeholders (offsite organizations, vendors, suppliers, regulatory authorities, and insurance companies) to understand their issues and concerns.
- Work with U.S. federal or state emergency management administrators or authorities to obtain the needed help and assistance during a disaster or incident in a timely manner.
- Familiarize yourself with management of alternate recovery sites (e.g., hot, cold, or warm sites) to understand their operations, policies, and procedures.

(d) Relationship of Business Continuity Management to ISO Standards

ISO standard 22301 focuses on BCM systems and requirements in order to prepare for, to protect against, and to reduce the likelihood of occurrence of disasters or disruptive incidents (i.e., man made, nature made, or technology used). The goal is to respond to and recover from disasters and incidents and to improve business continuity capabilities. Organizations are able to obtain certification to ISO 22301 similar to other certifiable standards, such as ISO 9000, ISO 14000, ISO 27001, and ISO 28000. Note that the standard previously known as British Institute's BS25999 standard has been transitioned to the ISO 22301 standard.

Other ISO standards related to BCM include ISO 15489, which provides general guidance regarding records management, and ISO 13606, which provides guidance regarding electronic health record communications.

6.5 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Authorization controls are a part of which of the following?

a. Directive controls

b. Preventive controls

c. Detective controls

d. Corrective controls

2. Which of the following is **not** an example of nondiscretionary access control?

a. Identity-based access control

b. Mandatory access control

c. Role-based access control

d. Temporal constraints

3. Which of the following statements are true about access controls, safety, trust, and separation of duty?

I. No leakage of access permissions are allowed to an unauthorized principal.

II. No access privileges can be escalated to an unauthorized principal.

III. No principals' trust means no safety.

IV. No separation of duty means no safety.

a. I only

b. II only

c. I, II, and III

d. I, II, III, and IV

4. For privilege management, which of the following is the correct order?

a. Access control → Access management → Authentication management → Privilege management

b. Access management → Access control → Privilege management → Authentication management

c. Authentication management → Privilege management → Access control → Access management

d. Privilege management → Access management → Access control → Authentication management

5. The encryption technique that requires two keys, a public key that is available to anyone for encrypting messages and a private key that is known only to the recipient for decrypting messages, is

a. Rivest, Shamir, and Adelman (RSA).

b. Data encryption standard (DES).

c. Modulator-demodulator.

d. A cipher lock.

6. The use of message encryption software:

a. Guarantees the secrecy of data.

b. Requires manual distribution of keys.

c. Increases system overhead.

d. Reduces the need for periodic password changes.

7. The information systems and audit directors agreed on the need to maintain security and integrity of transmissions and the data they represent. The best means of ensuring the confidentiality of satellite transmissions would be:

a. Encryption.

b. Access control.

c. Monitoring software.

d. Cyclic redundancy checks.

8. For application user authenticator management purposes, use of which of the following is risky and leads to stronger alternatives?

a. A single sign-on mechanism

b. Same user identifier and different user authenticators on all systems

c. Same user identifier and same user authenticator on all systems

d. Different user identifiers and different user authenticators on each system

9. Which of the following statements is **true** about intrusion detection systems (IDSs) and firewalls?

a. Firewalls are a substitute for an IDS.

b. Firewalls are an alternative to an IDS.

c. Firewalls are a complement to an IDS.

d. Firewalls are a replacement for an IDS.

10. Which one of the following is **not** an authentication mechanism?

a. What the user knows

b. What the user has

c. What the user can do

d. What the user is

11. Which of the following is the correct sequence of steps to be followed in an application software change control process?

I. Test the changes.

II. Plan for changes.

III. Initiate change request.

IV. Release software changes.

a. I, II, III, and IV.

b. II, I, III, and IV.

c. III, II, I, and IV.

d. IV, III, I, and II.

12. Software configuration management (SCM) should primarily address which of the following questions?

a. How does software evolve during system development?

b. How does software evolve during system maintenance?

c. What constitutes a software product at any point in time?

d. How is a software product planned?

13. Security controls are designed and implemented in which of the following system development life cycle (SDLC) phases?

a. Planning/initiation

b. Development/acquisition

c. Implementation/assessment

d. Disposal/decommissioning

14. Which of the following tests is driven by system requirements?

a. Black box testing

b. White box testing

c. Gray box testing

d. Glass box testing

15. Which of the following volatile data generated by operating system software installed on workstations and servers should be collected first prior to conducting computer forensic auditing work?

I. Network connections

II. Login sessions

III. Network configuration

IV. Operating system time

a. I and II.

b. I and III.

c. II and III.

d. III and IV.

16. Which of the following are the potential advantages of using cloud computing technology to user organizations?

I. They can access data and documents from anywhere and at any time.

II. They can reduce the cost of purchasing additional hardware and software.

III. They can reduce the cost of purchasing additional storage memory devices.

IV. They can implement pay-as-you-go method.

a. I and II.

b. I and IV.

c. I and III.

d. I, II, III, and IV.

17. Which of the following statements is **not** true? A data warehouse is:

a. Distributed.

b. Subject oriented.

c. Time variant.

d. Static in nature.

18. Which of the following provides an effective security control over the Internet access points or hot spots during remote access and telework?

a. Virtual private network

b. Wireless personal area network

c. Wireless local area network

d. Virtual local area network

19. What does an effective backup method for handling large volumes of data in a local area network (LAN) environment include?

a. Backing up at the workstation.

b. Backing up at the file server.

c. Using faster network connection.

d. Using Redundant Array of Independent Disks technology.

20. All of the following are examples of security risks over servers **except**:

a. Client/server architecture.

b. Data concentration.

c. Attack targets.

d. A single point of failure.

21. Which of the following server types is used for protection from malicious code attacks at the network gateway?

a. A web server

b. An image server

c. A mail server

d. A quarantine server

22. Which of the following information technology contingency solutions for servers minimizes the recovery time window?

a. Electronic vaulting

b. Remote journaling

c. Load balancing

d. Disk replication

23. Contingency plans for information technology operations should include appropriate backup agreements. Which of the following arrangements would be considered too vendor dependent when vital operations require almost immediate availability of computer resources?

a. A hot site arrangement

b. A cold site arrangement

c. A cold and hot site combination arrangement.

d. Using excess capacity at another data center within the organization

24. From an operations viewpoint, the **first step** in contingency planning is to perform a(n):

a. Operating system software backup.

b. Applications software backup.

c. Documentation backup.

d. Hardware backup.

25. The primary contingency strategy for application systems and data is regular backup and secure offsite storage. From an operations viewpoint, which of the following decisions is **least** important to address?

a. How often the backup is performed

b. How often the backup is stored offsite

c. How often the backup is used

d. How often the backup is transported

DOMAIN 7

Financial Management (13–23%)

7.1 Financial Accounting and Finance

Various topics are included in this section, including those listed next.

- Basic concepts
- Intermediate concepts
- Advanced concepts
- Financial statement analysis
- Types of debt and equity
- Financial instruments
- Cash management
- Valuation models
- Capital budgeting methods and decisions
- Cost of capital evaluations
- Taxation schemes
- Mergers, acquisitions, and divestitures

(a) Basic Concepts and Underlying Principles of Financial Accounting

Financial accounting (FA) is the language of business. All business transactions eventually end up in financial statements. Accounting principles are used to classify, record, post, summarize, and report the business transactions among various parties involved. Accountants apply their professional standards to analyze business transactions, prepare estimations, and report business events. The business transactions data accumulated in the chart of accounts are used to prepare

the financial statements of an organization. Accounting principles and qualities of accounting information, the accounting cycle, different formats of financial statements, and account analysis are discussed in this section.

(i) Accounting Principles and Qualities of Accounting Information

(A) Accounting Principles If company management could record and report financial data as it saw fit, comparisons among companies would be difficult, if not impossible. Thus, financial accountants follow generally accepted accounting principles (GAAP) in preparing reports. These reports allow investors and other stakeholders to compare one company to another.

Accounting principles and concepts are developed from research, accepted accounting practices, and pronouncements of authoritative bodies. Currently, the Financial Accounting Standards Board (FASB) is the authoritative body having the primary responsibility for developing accounting principles. The FASB publishes *Statements of Financial Accounting Standards* and *Interpretations* to these Standards.

Next, we emphasize accounting principles and concepts. It is through this emphasis on the "why" of accounting as well as the "how" that you will gain an understanding of the full significance of accounting. In the following paragraphs, we discuss the business entity concept, the cost concept, the matching concept, and other accounting concepts.

Business Entity Concept The individual business unit is the business entity for which economic data are needed. This entity could be an automobile dealer, a department store, or a grocery store. The business entity must be identified so that the accountant can determine which economic data should be analyzed, recorded, and summarized in reports.

The business entity concept is important because it limits the economic data in the accounting system to data related directly to the activities of the business. In other words, the business is viewed as an entity separate from its owners, creditors, or other stakeholders. For example, the accountant for a business with one owner (a proprietorship) would record the activities of the business only, not the personal activities, property, or debts of the owner. The business entity concept can be related to economic entity assumption, which states that economic activity can be identified with a particular unit of accountability; going-concern assumption, where the accountant assumes unless there is evidence to the contrary, that the reporting entity will have a life long enough to fulfill its objectives and commitments; and monetary unit assumption, where it provides that all transactions and events can be measured in terms of a common denominator—the dollar.

Cost Concept The historical cost concept is the basis for entering the *exchange price* or *cost of an asset* into the accounting records. Using the cost concept involves two other important accounting concepts: objectivity and the unit of measure. The objectivity concept requires that the accounting records and reports be based on objective evidence. In exchanges between a buyer and a seller, both try to get the best price. Only the final agreed-on amount is objective enough for accounting purposes. If the amounts at which properties were recorded were constantly being revised upward and downward based on offers, appraisals, and opinions, accounting reports would soon become unstable and unreliable. The unit of measure concept requires that economic data be recorded in dollars. Money is a common unit of measurement for reporting uniform financial data and reports.

Matching Concept The matching concept, which is based on accrual accounting, refers to the matching of expenses and revenues (hence net income) for an accounting period. Under the

accrual basis, revenues are reported in the income statement in which they are earned. Similarly, expenses are reported in the same period as the revenues to which they relate. Under the cash basis of accounting, revenues and expenses are reported in the income statement in the period in which cash is received or paid.

Other Accounting Concepts The materiality concept implies that errors, which could occur during journalizing and posting transactions, should be significant enough to affect the decision-making process. All material errors should be discovered and corrected. The accounting period concept breaks the economic life of a business into time periods and requires that accounting reports be prepared at periodic intervals. The revenue recognition concept, which is based on accrual accounting, refers to the recognition of revenues in the period in which they are earned.

(B) Qualities of Accounting Information The accounting function collects the raw data from business transactions and converts them into information useful to the decision maker. In this regard, the accounting information should contain two qualitative characteristics: primary and secondary qualities.

Primary Qualities The two primary qualities that distinguish useful accounting information are relevance and reliability. If either of these qualities is missing, accounting information will not be useful. "Relevance" means the information must have a bearing on a particular decision situation. Relevant accounting information possesses at least two characteristics: timeliness and predictive value or feedback value. "Timeliness" means accounting information must be provided in time to influence a particular decision. "Predictive value" means accounting information can be used to predict the future and timing of cash flows. "Feedback value" means the accounting function must provide decision makers with information that allows them to assess the progress or economic worth of an investment.

To be considered reliable, accounting information must possess three qualities: verifiability, representational faithfulness, and neutrality. Information is considered verifiable if several individuals, working independently, would arrive at similar conclusions using the same data. "Representational faithfulness" means accounting information must report what actually happened. "Neutrality" means accounting information must be free of bias or distortion.

Secondary Qualities The term "secondary qualities" does not mean that these characteristics are of lesser importance than the primary qualities. If a secondary characteristic is missing, the accounting information is not necessarily useless. The secondary qualities of useful information are comparability and consistency. "Comparability" means accounting reports generated for one firm may be easily and usefully compared with the accounting reports generated for other firms. If the two firms use totally different accounting methods, it would be very difficult to make a useful comparison of their data and information. "Consistency" means that a firm systematically uses the same accounting methods and procedures from one accounting period to the next accounting period.

In addition to the primary and secondary qualities, the accounting information must be understandable to economic decision makers. The earnings management strategy can destroy the primary and secondary qualities of accounting information.

(ii) Accounting Cycle

FA provides accounting information for use by those outside and inside the organization. This information is used by current and potential investors to determine the future benefits they will receive if they hold or acquire ownership in a business. Creditors and lenders use this information

to assess the creditworthiness of an organization. Other users of this information include employees, unions, customers, the general public, and governmental units.

Transactions, in accounting, are the result of the exchange of goods and/or services. Two factors allow the recording of a transaction: evidence and measurement. An exchange is an observable event and, therefore, provides evidence of business activity. This exchange takes place at a set price and, thus, provides an objective measure of the economic activity. The accounting cycle is one of four business cycles; the other three are sales, finance, and production.

With the traditional accounting model, a double-entry system of record keeping is used. The fundamental equation used with this system is

$$\text{Assets} = \text{Liabilities} + \text{Owners' equity}$$

All transactions are analyzed and then recorded based on their effect on assets, liabilities, and owners' equity. The increases and decreases in these accounts are recorded as debits or credits. In recording these transactions, the total amount of debits must equal the total amount of credits. The requirement that debits and credits must be equal gives rise to the double-entry method of record keeping. The rules of debits and credits are listed next.

Debits	Credits
Increase assets	Decrease assets
Decrease liabilities	Increase liabilities
Decrease owners' equity	Increase owners' equity
Increase owners' drawing	Decrease owners' drawing
Decrease revenues	Increase revenues
Increase expenses	Decrease expenses

(A) Cash-Basis versus Accrual-Basis Accounting The two approaches of accounting are **cash-basis accounting** and **accrual-basis accounting**. With cash-basis accounting, revenues are recognized when cash is received, and expenses are recognized when cash is paid out. The primary advantages of cash-basis accounting are the increased reliability due to the fact that transactions are not recorded until complete and the simplicity due to the fact that fewer estimates and judgments are required.

For most businesses, cash-basis accounting for a period requires recognition and measurement of noncash resources and obligations. Cash-basis accounting is not in accordance with GAAP.

With accrual-basis accounting, revenues are recognized when sales are made or services are performed, and expenses are recognized as incurred. Revenues and expenses are recognized in the period in which they occur rather than when cash is received or paid out.

In accrual accounting, the financial effect of transactions that have cash consequences are recorded in the periods in which those transactions occur rather than in the periods in which cash is received or paid.

(B) Steps in the Accounting Cycle The accounting cycle records the effect of economic transactions on the assets, liabilities, and owners' equity of an organization. The accounting cycle involves the eight steps shown in Exhibit 7.1.

1. Analysis of transactions
2. Journalizing of transactions
3. Posting to ledger
4. Trial balance and working papers
5. Adjusting journal entries
6. Closing journal entries
7. Preparing financial statements
8. Reversing journal entries

EXHIBIT 7.1 Eight Steps in The Accounting Cycle

Analysis of Transactions Each transaction must be analyzed before being recorded to determine the effect on the assets, liabilities, and owners' equity accounts. Asset, liability, and equity accounts are known as **real** accounts because they are not closed at the end of an accounting period. Revenue and expense accounts, however, are referred to as **nominal** accounts because they are closed at the end of an accounting period (usually a year), and their balances are reduced to zero. Therefore, real accounts represent the financial position of an organization at any point in time. Nominal accounts represent the results of operations over a given period of time.

Journalizing of Transactions After analysis to determine the affected accounts, transactions are recorded in the accounting journal, or journalized. Each account affected, the amount of the changes, and the direction of the changes (increases or decreases) are recorded. These transactions are recorded in the general journal or special journals, which serve as a chronological record of all the economic transactions of an organization. Special journals group similar types of transactions to provide more efficient processing of data. These journals systematize the original recording of major recurring types of transactions, such as cash receipts, cash disbursements, purchases, and sales.

The general journal is used to make entries that do not fit in the special journals, to make adjusting entries at the end of the accounting period, and to make closing entries at the end of the accounting period.

Posting to the Ledger The ledger is the complete collection of all the accounts of an organization. Transactions are posted to individual ledger accounts after being journalized. The ledger maintains the current balance of all the accounts.

Most organizations maintain subsidiary ledgers for accounts receivable (A/R) and accounts payable (A/P),because it is difficult to determine amounts due from specific customers and amounts due to specific suppliers using the master A/R account in the ledger. When using subsidiary ledgers, entries to the general ledger are totals for a specific period of time—for example, weekly totals—from the special journals. The sums of all subsidiary ledgers should be equal to the master account in the general ledger.

Trial Balance and Working Papers Working papers are large columnar sheets of paper for entering and summarizing the information necessary for making adjusting and closing entries

and preparing financial statements. Working papers are prepared at the end of an accounting period and are for internal use only.

The first step in the preparation of working papers is the preparation of a trial balance. The trial balance lists all accounts with balances as of the end of the accounting period. Account balances are entered in the columns and totaled. If postings for the period are arithmetically correct, then debits will equal credits. The trial balance does not provide a means of determining whether transactions have been posted to the correct accounts or journalized and/or posted to the general journal.

Adjusting Journal Entries With the accrual system of accounting, certain adjustments must be made at the end of each accounting period. These adjusting entries convert the amounts actually in the accounts to the amounts that should be in the accounts for proper financial reporting. These adjusting entries allocate the cost of assets used in several accounting periods and revenues earned in several accounting periods, accrue revenues and expenses attributable to the current period that have not been recorded, and make appropriate end of period adjustments in the carrying value of certain assets (i.e., marketable securities and inventories).

With accrual accounting, the cost of long-term assets must be apportioned to the periods that benefit from their use. The three types of long-term assets are **productive** assets, such as buildings and machinery, **wasting** assets, such as minerals, and **intangible** assets, such as patents and copyrights. These assets are apportioned to periods through depreciation, depletion, and amortization.

Another type of revenue and expense apportionment is to record the portion of unearned revenues earned during the year and the portion of a prepaid expense that expired during the year. Three steps are necessary to make adjusting entries:

1. Determine the current balance in an account.
2. Determine the appropriate balance for the account.
3. Make the appropriate entry or entries to achieve the desired ending balances.

An adjusting entry may be necessary to reduce an asset to its market value. Some common adjustments are A/R, inventories, and marketable securities. These accounts are adjusted by debiting an expense or loss account and crediting a contra asset account.

Closing Journal Entries After posting adjusting entries, all nominal accounts with existing balances are closed to **real** accounts. These closing entries reduce the nominal account balances to zero to show the effect of these accounts on owners' equity and so that information for the next accounting period may be accumulated. Three steps are required:

1. Close all revenue, gain, expense, and loss accounts to the expense and revenue summary account. This account is used only at the end of an accounting period to summarize revenues and expenses for the period.
2. Close the expense and revenue summary account to retained earnings.
3. Close the dividend account to retained earnings.

A postclosing trial balance is prepared after making all necessary closing entries. This provides a check against partial posting of closing entries. The postclosing trial balance reflects the balances to be included in the balance sheet at the end of the period.

Preparing Financial Statements After preparing the adjusting entries and posting them to the working papers, an income statement can be prepared using the income statement numbers from the working papers.

After preparing the closing entries and posting them to the working papers, the only accounts with balances should be the asset, liability, and owners' equity accounts. At this time, a statement of stockholders' equity or statement of retained earnings should be prepared. This statement summarizes the transactions affecting the owners' capital account balance or retained earnings. Such a statement shows the beginning capital account, plus net income or less net loss, less owners' withdrawals or dividends. The ending capital account is then carried forward to the balance sheet, which helps to relate income statement information to balance sheet information.

Now it is time to prepare the balance sheet. The balance sheet is divided into assets, liabilities, and owners' equity and reflects the balances in these accounts at the end of the year.

Reversing Journal Entries Reversing entries, the final step in the accounting cycle, are recorded on the first day of the next accounting period. Reversing entries are prepared to reverse the effects of certain adjusting entries to which they relate. These entries reduce the possibility of including a revenue or expense at the time of the adjusting entry and including it again when the economic transaction occurs. The general rule on reversing entries is that all adjusting entries that increase assets or liabilities may be reversed. Therefore, the only adjusting entries that should be reversed are those that accrue revenues or expenses. Reversing entries are optional and are dependent on an organization's bookkeeping system.

Examples of Journal Entries

Next we present varied examples of journal entries for better understanding of recording of business transactions with accounting implications.

Example 1

Debiting the prepaid insurance account and crediting the accounts payable account would correctly record the purchase of a liability insurance policy on account.

Example 2

Debiting the interest expense account and crediting the interest payable account would correctly record the accrued expense transaction.

Example 3

A company has been sued for $100 million for producing and selling an unsafe product. Attorneys for the company cannot predict the outcome of the litigation. In its financial statements, the company should disclose the existence of the lawsuits in a footnote without making a journal entry. The situation did not meet the criteria for setting up as a contingent liability. Only disclosure is required when a loss contingency is possible. No accrual is required because the loss could not be reasonably estimated.

Example 4

In the December 31, 2010, balance sheet, ending inventory was valued at $140,000. An investigation revealed the true balance should have been $150,000. In the December 31, 2011, balance sheet, ending inventory was shown at $200,000. The correct balance should have been $180,000. All errors were discovered during an investigation in 2012 before the books were closed. Ignoring tax effects, the appropriate journal entry that should be made in 2012 to correct the errors would be debiting the retained earnings for $20,000 to correct the decreased income and crediting the inventory for $20,000 to correct the decreased inventory.

This is an example of **counterbalancing error** affecting both the balance sheet and the income statement. An entry to adjust the beginning balance of the retained earnings is necessary as it takes two years for the error to be counterbalanced naturally. Note that the books were not closed for 2012.

Example 5

A retail shoe store purchases a copy machine for its office. The copier is priced at $5,000. The store gives cash of $2,000 and a 10% one-year promissory note in exchange for the copier. The acquisition of the copy machine could be recorded by debiting the office equipment account, crediting the cash account for $2,000, and crediting the note payable account for $3,000.

The 10% interest rate seems reasonable and the note can be recorded at its face value since it is only for one year. Otherwise, present value (PV) should be used to record the note.

Example 6

A retail company purchases advertising services on account. The appropriate journal entry to record the purchase would be debiting the advertising expense account and crediting the accounts payable account.

Example 7

A company allows customers to redeem 20 coupons for a toy (cost $3.00). Estimates are that 40% of coupons distributed will result in redemption. Since beginning the promotion this year, 4 million coupons were distributed and 1 million redeemed. The adjusting journal entry to accrue for unredeemed coupons at year-end is debiting premium expense account for $90,000 and crediting estimated liability for premiums account for $90,000.

All expenses must be accrued at the end of accounting (fiscal) year. In this case, all unredeemed coupons that are still outstanding at year-end must be accrued. The liability of $90,000 is calculated as follows:

Unredeemed coupons are $4{,}000{,}000 \times 0.40 - 1{,}000{,}000 = 600{,}000$

Equivalent toys are $600{,}000/20 = 30{,}000$ toys

Liability is 30,000 toys × $3.00 cost per toy = $90,000

Example 8

The debit to supplies and credit to supplies expense is indication of an end-of-period adjusting journal entry. These adjustments may include inventory adjustments.

Example 9

When a perpetual inventory system is used and a difference exists between the perpetual inventory amount balance and the physical inventory count, the following journal entry is needed to adjust the perpetual inventory amount: A debit to inventory over and short account and a credit to inventory. A write-down of inventory has occurred, which is reported as an adjustment of cost of goods sold (COGS) or as another expense on the income statement.

(iii) Different Formats of Financial Statements

A full set of four financial statements discussed in this section is based on the concept of financial capital maintenance. For a period, the full set should show:

1. Financial position at the end of the period.
2. Earnings and comprehensive income for the period.
3. Cash flows during the period.
4. Investments by and distributions to owners during the period.

A statement of financial position provides information about an entity's assets, liabilities, and equity and their relationships to each other at a moment in time. The statement delineates the entity's resources structure—major classes and amounts of assets—and its financial structure—major classes and amounts of liabilities and equity.

A statement of financial position does not purport to show the value of a business enterprise but, together with other financial statements and other information, should provide information that is useful to those who desire to make their own estimates of the enterprise's value. Those estimates are part of financial analysis, not of financial reporting, but FA aids financial analysis.

Statements of earnings and of comprehensive income together reflect the extent to which and the ways in which the equity of an entity increased or decreased from all sources other than transactions with owners during a period.

The concept of earnings in these statements is similar to net income for a period in present practice; however, it excludes certain accounting adjustments of earlier periods that are recognized in the current period—cumulative effects of a change in accounting principle is the principal example from present practice. *Other names given to earnings are net income, profit, or net loss.*

The next list presents different meanings of the term "earnings."

- **Earnings** are a measure of entity performance during a period. They measure the extent to which assets inflows (revenues and gains) associated with cash-to-cash cycles substantially completed during the period exceed asset outflows (expenses and losses) associated, directly or indirectly, with the same cycle.
- **Comprehensive income** is a broad measure of the effects of transactions and other events on an entity. It comprises all recognized changes in equity (net assets) of the entity during a period from transactions and other events and circumstances except those resulting from investments by owners and distributions to owners. *Other names given to comprehensive income include total nonowner changes in equity or comprehensive loss.*
- Earnings and comprehensive income are **not** the same. Certain gains and losses are included in comprehensive income but are excluded from earnings. Those items fall into two classes that are illustrated by certain present practices: (1) effects of certain accounting adjustments of earlier periods that are recognized in the current period; and (2) certain other changes in entity assets (principally certain holding gains and losses) that are recognized in the period but are excluded from earnings, such as some changes in market values of investments in marketable equity securities classified as noncurrent assets, some changes in market values of investments in industries having specialized accounting practices for marketable securities, and foreign currency translation adjustments.

A **statement of cash flows** (SCF) directly or indirectly reflects an entity's cash receipts classified by major sources and its cash payments classified by major uses during a period, including cash flow information about its operating, financing, and investing activities.

A **statement of investments by and distributions to owners** reflects an entity's capital transactions during a period—the extent to which and in what ways the equity of the entity increased or decreased from transactions with investors as owners. Exhibits 7.2 through 7.5 present each of these four statements.

EXHIBIT 7.2 Statement of Financial Position

The statement of financial position (balance sheet) presents assets, liabilities, and shareholders' equity. The balance sheet provides a basis for assessing the liquidity and financial flexibility of an entity, computing rates of return on investments, and evaluating the capital structure of an entity. It reflects the financial status (health) of an enterprise in conformity with GAAP. The balance sheet reports the aggregate (and cumulative) effect of transactions at a point in time, whereas the statement of income, statement of retained earnings, and statement of cash flows report the effect of transactions over a period of time. The balance sheet is based on historical cost, the exchange price principle, or at the acquisition price.

Assets are classified as "current" if they are reasonably expected to be converted into cash, sold, or consumed either in one year or in the operating cycle, whichever is longer.

Liabilities are classified as "current" if they are expected to be liquidated through the use of current assets or the creation of other current liabilities.

Shareholders' equity arises from the ownership relation and is the source of enterprise distribution to the owners. Equity is increased by owners' investments and comprehensive income and is reduced by distributions to the owners.

Limitations of the balance sheet are listed next.

- It does not reflect current values. Items are recorded at a mixture of historical cost and current values. Historical cost used to record assets and liabilities does not always reflect current value. Monetary assets such as cash, short-term investments, and receivables closely approximate current values. Similarly, current liabilities closely approximate current value and should be shown on the balance sheet at face value.
- Fixed assets are reported at cost less depreciation, depletion, or amortization. Inventories and marketable equity securities are exceptions to historical cost, where they are allowed to be reported at lower of cost or market. Similarly, certain long-term investments, which are another exception, are reported under the equity method. Long-term liabilities are recorded at the discounted value of future payments.
- Judgments and estimates are used to determine the carrying value or book value of many assets. Examples include determining the collectibility of receivables, salability of inventory, and useful life of fixed (long-term) assets. Estimations are not necessarily bad; however, there is no accounting guidance available.
- Appreciation of assets is not recorded except when realized through an arm's-length transaction.
- Internally generated goodwill, customer base, managerial skills and talent, reputation, technical innovation, human resources, and secret processes and formulas are not recorded in the balance sheet. Only assets obtained in a market transaction are recorded.
- It ignores the time value of its elements. Most items are stated at face value regardless of the timing of the cash flows that they will generate. Exceptions are certain long-term receivables and payables, which are discounted.
- It omits off–balance sheet items (mostly liabilities), such as sales of receivables with recourse, leases, throughput arrangements, and take-or-pay contracts.

Classification of assets. In order to properly value an asset on the balance sheet, any related valuation allowance account should be reported contra to the particular asset account. Assets include current assets, noncurrent assets, and other assets.

Current assets include cash, short-term investments, receivables, inventories, and prepaid expenses. The key criterion as to whether something should be included in current assets is the length of the operating cycle. When the cycle is less than one year, the one-year concept is used. When the cycle is

very long, the usefulness of the concept of current assets diminishes. Specific components of current assets are listed next.

- **Cash and cash equivalents** include cash on hand consisting of coins, currency, undeposited checks, money orders and drafts, and deposits in banks. Certificates of deposit are not considered cash because of the time restrictions on withdrawal. Cash that is restricted in use or cash restricted for a noncurrent use would not be included in current assets. Cash equivalents include: short-term, highly liquid investments that are readily convertible to known amounts of cash and are near their maturity period; Treasury bills; commercial paper; and money market funds.
- **Short-term investments** are readily marketable securities acquired through the use of temporarily idle cash.
- **Receivables** include accounts receivable and notes receivable, receivables from affiliates, and receivables from officers and employees. Allowances due to uncollectibility and any amounts discounted or pledged should be clearly stated.
- **Inventories** are goods on hand and available for sale. The basis of valuation and the methods of pricing should be disclosed.
- **Prepaid expenses** are assets created by the prepayment of cash or incurrence of a liability. They expire and become expenses with the passage of time, usage, or events. Examples include prepaid rent, insurance, and deferred taxes.

Noncurrent assets include long-term investments; property, plant, and equipment; and intangible assets. Specific components are listed next.

- **Long-term investments** include investments that are intended to be held for longer than one operating cycle. Examples are debt and equity securities, tangible assets, investments held in sinking funds, pension funds, amounts held for plant expansion, and cash-surrender values of life insurance policies.
- **Property, plant, and equipment** includes machinery and equipment, buildings, furniture and fixtures, natural resources, and land. These assets are of a durable nature that are to be used in the production or sale of goods, sale of other assets, or rendering of services.
- **Intangible assets** include goodwill, trademarks, patents, copyrights, and organizational costs. Generally, the amortization of an intangible asset is credited directly to the asset account, although it is acceptable to use an accumulated amortization account.

Other assets include accounts that do not fit in the preceding asset categories. Examples include long-term prepaid expenses, deferred taxes, bond issue costs, noncurrent receivables, and restricted cash.

Classification of liabilities. The liabilities are presented in the balance sheet in the order of payment. They are grouped into three categories: current, noncurrent, and other.

Current liabilities include obligations arising from the acquisition of goods and services entering the operating cycle, collections of money in advance for the future delivery of goods or performance of services, and other obligations maturing within the current operating cycle to be met through the use of current assets. **Exceptions** that are treated as noncurrent liabilities are debt expected to be refinanced through another long-term issue after the balance sheet date but prior to the issuance of the balance sheet and debt that will be retired through the use of noncurrent assets (bond sinking fund). The reason is that liquidation does not require the use of current assets or the creation of other current liabilities. The excess of total current assets over the current liabilities is called "working capital." Working capital provides a margin of safety or liquid buffer available to meet the financial demands of the operating cycle.

Noncurrent liabilities include obligations arising through the acquisition of assets, obligations arising out of the normal course of operations, and contingent liabilities involving uncertainty as to possible losses.

Other liabilities include deferred charges, noncurrent receivables, intangible assets, deferred income taxes, and deferred investment tax credits.

Classification of shareholders' equity. Shareholders' equity is the interest of the stockholders in the assets of an enterprise. It shows the cumulative net results of past transactions. Specific components are listed next.

- **Capital stock** consists of par/stated value of common and preferred stock.
- **Additional paid-in capital** includes: paid-in capital in excess of par/stated value, which is the difference between the actual issue price and par/stated value; paid-in-capital stock from other transactions, which includes treasury stock, retirements of stock, stock dividends recorded at market, lapse of stock purchase warrants, and conversion of convertible bonds in excess of the par value of the stock.
- **Donated capital** includes donations of noncash property such as land, securities, buildings, and equipment by either stockholders or outside parties.
- **Retained earnings** are accumulated earnings not distributed to the shareholders. They are divided into appropriated (certain amount is not available for dividends) and unappropriated (available for dividends).
- **Treasury stock** represents issued shares reacquired by the issuer. Treasury stock is stated at its cost of acquisition and as a reduction of shareholders' equity.
- **Adjustments of equity** include net unrealized losses on noncurrent portfolios of marketable equity securities, the excess of minimum pension liability over unrecognized prior service cost, and unrealized gains or losses on foreign currency transactions.

EXHIBIT 7.3 Statement of Income

The statement of income, also known as the income statement, statement of earnings, or statement of operations, summarizes the results of an entity's economic activities or performance for a period of time (i.e., an accounting period). It also measures a firm's profitability over a specific period. Enterprise management refer to the income statement to determine how efficiently or effectively resources are used and how investors and creditors view the income statement.

Forms of Income Statement

- Single step
- Multiple step
- Condensed

Many accountants prefer the single-step form of income statement with two groups: revenues and expenses. The **single-step** income statement is simple to present, and all items within expenses and revenues are treated similarly in terms of priorities. Expenses are deducted from revenues to arrive at net income or loss, hence the name "single step." One exception is income taxes, which are reported separately as the last item.

However, some accountants prefer a **multiple-step** income statement to present more information and to show better relationships with many classifications. The multiple-step statement separates operating transactions from nonoperating transactions and matches costs and expenses with related revenues. For example, the multiple-step income statement further classifies the item "administrative expenses" from the single-step income statement into office salaries, officers' salaries, utilities expenses, depreciation of buildings, and so on. Similarly, it breaks down the item "interest expenses" into interest on bonds, interest on notes, and so forth. Income taxes can be broken into current and deferred.

An unrealized loss resulting from a temporary decline in the market value of short-term investments in marketable equity securities should be reported as another expense or loss item on the multiple-step income statement. The short-term investments in marketable equity securities are carried at the lower of aggregate cost or market. The excess of aggregate cost over market is credited to a valuation account. Any increase in the valuation allowance is reported as a charge to income. These unrealized losses do not meet the criteria for classification as extraordinary and are not to be handled as prior-period adjustments. Unrealized losses on noncurrent marketable equity securities are to be classified as contra stockholders' equity.

The major distinction between the multiple-step and single-step income statement formats is the separation of operating and nonoperating data.

A condensed income statement presents, in addition to revenue, only the totals of expense groups, which it supports with supplementary schedules. These schedules can be found in the notes to the income statement.

An example of income statement sections in the order of presentation follows.

Income Statement Sections

1. Operating section
2. Nonoperating section
3. Income from continuing operations before income taxes
4. Income taxes
5. Income from continuing operations
6. Results from discontinued operations (gain/loss)
7. Extraordinary items (gain or loss)
8. Cumulative effect of a change in accounting principle
9. Net income
10. Earnings per share

Single-step income statements report irregular transactions, such as items 6 through 8, separately following income from continuing operations.

Limitations of income statements are presented next.

- Items that cannot be quantified with any degree of reliability are not included in determining income (i.e., economic income versus accounting income).
- Income numbers are often affected by the accounting methods employed (e.g., depreciation).
- Increases in income may result from a nonoperating or nonrecurring event that is not sustainable over a period of time (e.g., onetime tax forgiveness, exchange of preferred stock).

Limitations of accrual-based accounting for earnings are listed next.

- Information about the liquidity and potential cash flows of an organization is absent.
- The income statement does not reflect earnings in current dollars.
- Estimates and judgments must be used in preparing the income statement.

Major Components of the Income Statement

The major components and items required to be presented in the income statement include: income from continuing operations, results from discontinued operations, extraordinary items, accounting changes, net income, and earnings per share.

1. **Income from continuing operations**

   Sales or revenues are charges to customers for the goods and/or services provided during the period. Both gross and net sales/revenues should be presented by showing discounts, allowances, and returns.

   Cost of goods sold is the cost of the inventory items sold during the period for a manufacturing or retail company.

   Operating expenses are primary recurring costs associated with business operations to generate sales or revenues. It does not include cost of goods sold, but includes selling expenses (e.g., salesperson salaries, commissions, advertising) and general and administrative expenses (e.g., salaries, office supplies, telephone, postage, utilities, accounting and legal services). An expense is to be recognized whenever economic benefits have been consumed.

   Gains and losses stem from the peripheral transactions of the enterprise. Examples are write-downs of inventories and receivables, effects of a strike, and foreign currency exchange gains and losses.

   Expenses versus losses. Losses result from peripheral or incidental transactions whereas expenses result from ongoing major or central operations of the entity. Expense accounts are costs related to revenue whereas loss accounts are not related to revenue.

   Other revenues and expenses are revenues and expenses not related to the operations of the enterprise. Examples include gains and losses on the disposal of equipment, interest revenues and expenses, and dividend revenues. A material gain on the sale of a fully depreciated asset should be classified on the income statement as part of other revenues and gains. Since the sale of an asset is not an operating item, it should be classified as other revenues and gains.

   Income tax expense related to continuing operations.

2. **Results from discontinued operations.** It contains two components.

   The first component, income (loss) from operations, is disclosed for the current year only if the decision to discontinue operations is made after the beginning of the fiscal year for which the financial statements are being prepared.

   The second component, gain (loss) on the disposal, contains income (loss) from operations during the phase-out period and gain (loss) from disposal of segment assets. Discontinued operations are presented after income from continuing operations and before extraordinary income on the income statement. The disposal of a line of business is normal, and any loss should be treated as an ordinary loss.

3. **Extraordinary items.** Per Accounting Principles Board (APB) Opinion 30, two criteria must be met to classify an event or transaction as an extraordinary item: unusual nature (high degree of abnormality, clearly unrelated to, or only incidentally related to) and infrequency of occurrence (not reasonably be expected to recur in the foreseeable future). Various Statements of Financial Accounting Standards (SFAS)(required these **exceptional items** to be presented as extraordinary even though they do not meet the criteria stated above. (Remember that SFAS override the APB Opinions.)

   - Material gains and losses from the extinguishment of debt except for sinking-fund requirements
   - Profit or loss resulting from the disposal of a significant part of the assets or a separable segment of previously separate companies, provided the profit or loss is material and the disposal is within two years after a pooling of interest
   - Write-off of operating rights of motor carriers
   - The investor's share of an investee's extraordinary item when the investor uses the equity method of accounting for the investee
   - Gains of a debtor related to a troubled debt restructuring

   Extraordinary items should be segregated from the results of ordinary operations and be shown net of taxes in a separate section of the income statement, following discontinued operations

and preceding cumulative effect of a change in accounting principle. Extraordinary losses must be both unusual and nonrecurring. Sales price minus net book value is gain or loss. A loss because of an expropriation of assets by a foreign government is classified as an extraordinary item in the income statement.

APB 28 requires that extraordinary items be disclosed separately and included in the determination of net income for the interim period in which they occur. Extraordinary gain should not be prorated or loss should not be deferred.

4. **Accounting changes.** A change in accounting principles (including methods of applying them) results from adoption of a GAAP different from the one previously used for reporting purposes. The effect on net income of adopting the new accounting principle should be disclosed as a separate item following extraordinary items in the income statement. Changes in accounting estimates (lives of fixed assets, adjustments of the costs) are not considered errors or extraordinary items; instead, they are considered prior-period adjustments.
5. **Net income.** Obviously, net income is a derived item by subtracting results from discontinued operations, extraordinary items, and cumulative effect of changes in accounting principles from income from continuing operations.
6. **Earnings per share.** Earnings per share (EPS) is a compact indicator of a company's financial performance. It is used to evaluate a firm's stock price, assess the firm's future earnings potential, and determine the firm's ability to pay dividends. EPS is calculated as net income minus preferred dividends divided by the weighted average of common shares outstanding. EPS must be disclosed on the face of the income statement. EPS may be disclosed parenthetically when only a one per-share amount is involved.

   EPS must be reported for the following items:

- Income from continuing operations
- Income before extraordinary items and cumulative effect of changes in accounting principles
- Cumulative effect of changes in accounting principles
- Net income
- Results from (gain/loss on) discontinued operations (optional)
- Gain or loss on extraordinary items (optional)

Example of Single-Step Income Statement

Revenues
Net sales
Dividend revenue
Rental revenue
  Total revenues
Expenses
COGS
Selling expenses
Administrative expenses
Interest expense
Income tax expense
Total expenses
  Net income
  Earnings per common share

Example Calculation of Purchasing Power Gain or Loss on Net Monetary Items

A corporation has gathered the following data in order to compute the purchasing power gain or loss to be included in its supplementary information for the year ended December 31, 20X1:

Amount in nominal dollars		
	December 31, 20X0	December 31, 20X1
Net monetary assets	$800,000	$943,000

	Index number
Consumer price index at December 31, 20X0	200
Consumer price index at December 31, 20X1	230
Average consumer price index for 20X1	220

Question: What is the purchasing power gain or loss on net monetary items (expressed in average-for-the-year dollars for 20X1) reported at what amount for the year ended December 31, 20X1?

Answer: $121,000 purchasing power loss, as shown below.

The net monetary asset position at the beginning of the period ($800,000) is restated to $880,000 average constant dollars ($800,000 × 220/200 = $880,000). The actual increase in net monetary assets ($943,000 – $800,000 = $143,000) is assumed to have occurred evenly throughout the year so it is already stated in terms of average-for-the-year dollars. The restated beginning balance ($880,000) plus the increase ($143,000) yields a subtotal of $1,023,000. This subtotal is compared with the ending balance restated to an average basis ($943,000 × 220/230 = $902,000) to yield a purchasing power loss of $121,000.

The statement of retained earnings is a reconciliation of the balance of the retained earnings account from the beginning to the end of the year. This statement tells the reader how much money management is plowing back into the business. Prior-period adjustments, including correction of errors (net of taxes), are charged or credited to the opening balance of retained earnings.

Net income is added and dividends declared are subtracted to arrive at the ending balance of retained earnings. This statement may report two separate amounts: retained earnings free (unrestricted) and retained earnings appropriated (restricted). Statement of Financial Accounting Standards (SFAS) 16, *Prior Period Adjustments*, provides additional guidelines.

The statement of income and the statement of retained earnings can be shown separately. It is an acceptable practice to combine them into a single statement called the statement of income and retained earnings for convenience. Net income is computed in the same manner as in a multiple- or single-step income statement. The beginning balance in retained earnings is added to the net income (loss) figure. Any prior-period adjustments are included in the retained earnings to obtain adjusted retained earnings. Declared dividends (for both preferred stock and common stock) are deducted to obtain the retained earnings ending balance.

EXHIBIT 7.4 Statement of Retained Earnings

Example of Retained Earnings Statement

Retained earnings balance at the beginning of the period
Prior period adjustments, net of taxes (+/–)
Correction of an error, net of taxes (+/–)
Net income (+)
Dividends declared (–)
Retained earnings balance at the end of the period

EXHIBIT 7.5 Statement of Cash Flows

The statement of cash flows (SCF) replaces the previous statement of changes in financial position. The primary purpose of the SCF is to provide relevant information about the cash receipts and cash payments of an enterprise during a period. A secondary purpose is to provide information about the investing and financing activities of the enterprise during the same period. The emphasis in the SCF is on gross cash receipts and cash payments. For example, the SCF is the most useful financial statement for a banker to evaluate the ability of a commercial loan customer to meet current obligations. Cash flow per share should not be reported in the financial statements. Foreign currency exchange rate effects should be used in the preparation of the consolidated SCF.

Noncash exchange gains and losses recognized on the income statement should be reported as a separate item when reconciling net income and operating activities. The SCF includes net income, depreciation, investing activities, financing activities, and operating activities.

Specifically, the SCF should help investors and creditors assess:

- Ability to generate future positive cash flows.
- Ability to meet obligations and pay dividends.
- Reasons for differences between income and cash receipts and cash payments.
- Both cash and noncash aspects of an entity's investing and financing transactions.

Classification

The statement of cash flows requires three classifications: investing activities, financing activities, and operating activities.

Investing activities show the acquisition and disposition of long-term productive assets or securities that are not considered cash equivalents. This category also includes the lending of money and collection of loans.

Financing activities include obtaining resources from and returning resources to the owners. This category also includes resources obtained from creditors and repaying the amount borrowed.

Operating activities include all transactions that are not investing and financing activities. This category includes delivering or producing goods for sale and providing services to customers. It involves cash effects of transactions that enter into the determination of net income for the period.

Although the Financial Accounting Standards Board (FASB) has expressed a preference for the direct method of presenting net cash from operating activities, the indirect method can also be used. The

direct method shows the items that affected cash flow. This method allows the user to clarify the relationship between the company's net income and its cash flows. It reports only the items that affect cash flow (e.g., real cash inflows and real cash outflows) and ignores items that do not affect cash flow (e.g., depreciation and gains).

Entities using the direct method are required to report the following classes of operating cash receipts and payments:

- Cash collected from customers
- Interest and dividend received
- Cash paid to employees and other suppliers
- Interest and income taxes paid
- Other operating cash receipts and payments

The **indirect method** of presenting net cash from operating activities is most widely used and easy to prepare. It focuses on the difference between net income and cash flows. It emphasizes changes in the components of most current asset and current liability accounts. The amount of interest and income tax paid should be included in the related disclosures. Depreciation expense should be presented as an addition to net income in converting net income to net cash flows from operating activities.

The following tables present examples of the SCF classifications in terms of cash inflows and cash outflows.

Cash Inflows

Operating	Investing	Financing
Cash receipts exceed cash expenditures	Principal collections from loans	Proceeds from issuing equity securities
Receipts from sale of goods or services	Sale of long-term debt or equity securities	Proceeds from issuing short-term or long-term debt (e.g., bonds, notes)
Returns on loans (interest)	Sale of property, plant, and equipment	
Returns on equity securities (dividends)		

Cash Outflows

Operating	Investing	Financing
Cash expenditures exceed cash receipts	Loans made to others	Payment of dividends
Payments for inventory	Purchase of long-term debt or equity securities	Repurchase of entity's capital stock (e.g., treasury stock)
Payments to employees	Purchase of property, plant, and equipment	Repayment of debt principal
Payments of taxes		
Payments of interest		
Payments to suppliers		

(iv) Account Analysis

Account analysis helps the internal auditor reconstruct balance sheet accounts from account balances and journal entries and understand the account classifications and posting error correction process through journal entries.

The composition of accounts with their balances and the nature of business transactions and their effect on account balances can be analyzed using two approaches: worksheet (columnar) approach and T-account approach (see Exhibit 7.6).

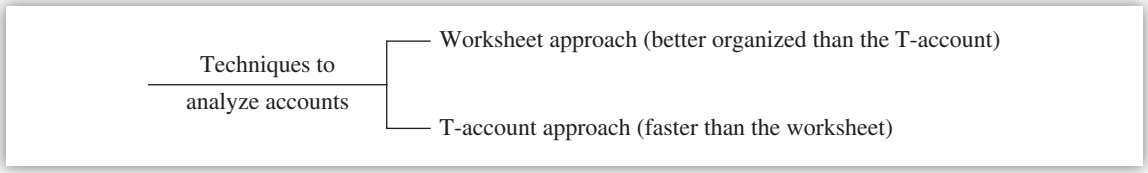


EXHIBIT 7.6 Techniques to Analyze Accounts

(A) Techniques to Analyze Accounts The **worksheet approach** analyzes the changes that occurred in the balance sheet accounts by considering the income statement items. This approach is better organized than the T-account approach.

The **T-account approach** analyzes the changes in the noncash accounts and provides details on the cash flows during the period. This approach is faster than the worksheet approach.

It should be noted that there will always be a cause-and-effect relationship between and among accounts due to interlinking of those accounts. Consideration should be given to the characteristics of accounts, such as the number of accounts affected, the time frame involved, and the nature of the effect.

At least two accounts will be related to each other, and usually more. For example, an income statement classification error has no effect on the balance sheet and no effect on net income.

The time horizons for these causes and effects to materialize would be the past, present, and future accounting periods, due to lagging and leading effects of accounts. For example, it takes two accounting periods to correct a counterbalancing error itself while it takes more than two periods to correct a noncounterbalancing error itself.

Two types of effects can be seen: direct and indirect. An example of direct effect is overstatement of net income when wage expense is understated. Liability being understated when wage expense is understated is an example of an indirect effect.

The internal auditor needs to understand account relationships when conducting audits, whether financial or operational. This understanding helps the auditor know what to look for during the account examination and verification process and how to conduct tracing and vouching work. This, in turn, will ensure that all related accounts and their effects are reviewed. Such account analysis will most likely help the auditor in reviewing the completeness, accuracy, and appropriateness of accounting journal entries and not so much who made the entries.

A partial, independent list of accounts with established interrelationships is presented next.

- The balance in inventory accounts will increase prior to sales while the balance in customer receivable accounts will increase after the sales. The reason is that adequate inventories

must be available in advance for sales to take place. Here sales, inventories, and receivable accounts are being affected.

- The effects of misstating unearned interest as revenue would overstate revenue and receivables for this period and understate revenue for later periods. Examples of accounts that would be affected include interest, receivables, and income.
- When receivables are collected, the balance in cash accounts rises and the balance in receivable accounts falls. Working capital, which is current assets minus current liabilities, stays the same. Here the working capital composition has just been rearranged. These transactions have an inverse effect on each other since only asset accounts with opposite change are involved.
- During recession, receivables will likely increase as customers attempt to squeeze their trade credit limits to the maximum. This, in turn, increases funds tied up in working capital. Such an increase in working capital would reduce available cash and increase the need for financing. Cash, receivables, and liabilities accounts are affected here.
- Equal changes in A/R and A/P would alter the balance of cash but have no affect on working capital. Here the change has an offsetting effect since receivables and payables move in the opposite direction of the balance sheet.
- Issuance of common stock will increase cash, thereby increasing working capital. Cash accounts, stock accounts, and liability accounts are involved here.
- The longer the sales cycle is, the more working capital required. This is an example of the effect on interrelationships among accounting cycles and accounts within a cycle. Here both sales cycle and finance cycle are affected.
- An increase in the average length of time to collect receivables from customers would increase bad debts for the same type of customers.
- If credit-granting policies become too strict, the company will lose customers. If inventory balances are reduced too much, stock-out costs will be increased. Both situations will result in lower profits to the company.
- The just-in-time (JIT) inventory concept minimizes working capital investment because the firm maintains only a minimum amount of inventory. This is a result of vendors continuously making small deliveries of raw materials and parts that are immediately used on the factory floor.
- Payment of the current portion of the mortgage payable would not affect the net working capital situation.

(b) Intermediate Concepts of Financial Accounting

(i) Bonds

(A) Overview Bonds result from a single agreement. However, a bond is intended to be broken up into various subunits. Notes and bonds have similar characteristics, including a written agreement stating the amount of the principal to be paid, the interest rate, when the interest and principal are to be paid, and the restrictive covenants.

The stated interest rate on a note or bond often differs from the market interest rate at the time of issuance. When this occurs, the PV of the interest and principal payments will differ from the maturity, or face value. Possible scenarios include:

- When the market rate exceeds the stated rate, the instrument is sold at a **discount**, meaning that the cash proceeds are less than the face value.
- When the stated rate exceeds the market rate, the instrument is sold at a **premium**, meaning that the cash proceeds are more than the face value.
- When the market and stated rates are the same at the time of issuance, no discount or premium exists, and the instrument will be sold at its face value.

The proper valuation is the PV of the future payments using the market rate of interest, either stated or implied in the transaction, at the date the debt was incurred.

EXCEPTIONS TO PRESENT VALUE OR MARKET INTEREST RATES

- Deferred income tax debits should not be discounted.
- Deferred income tax credits should not be discounted.
- Long-term notes should be valued using an imputed interest rate with no stated interest rate.

Nominal rate, stated rate, or coupon rate are all names for the interest rate stated on a bond. The periodic interest payments on a bond are determined by this rate. However, the price at which the bonds are sold determines the actual interest expense incurred on the bond issue. The actual rate of interest incurred is called the effective rate, yield rate, or market rate and is determined by the investment market.

When a bond sells at par value or face amount, the effective interest rate and the stated rate are equal. When a bond sells at a **discount** (below par), the effective rate is greater than the stated rate. When a bond sells at a **premium** (above par), the stated rate is greater than the effective rate of the bond; then the bond will sell at a discount. If the prevailing market rate of interest is less than the stated rate, then the bond will sell at a premium.

When a bond sells at a discount, a contra liability account, discount on bonds payable, is debited for the amount of the discount (excess of face value over cash proceeds). This contra liability account is shown as a deduction from bonds payable on the balance sheet. This discount is then amortized over the life of the bonds by one of two methods.

1. **Straight-line method.** Under this method, the amount to be amortized each period is determined by dividing the discount by the number of periods in the life of the bonds. Therefore, an equal amount of discount is charged to expense each period.
2. **Effective interest method.** This method computes bond interest expense for the period by multiplying the effective interest rate (at the bond issue date) by the bond's carrying value at the beginning of the period.

The difference between interest expense for the period and interest payable for the period is the discount amortized for the period.

The carrying value of the bonds issued at a discount increases as they mature. Therefore, the effective interest expense increases as the bonds mature, since it is based on the carrying value of the bonds.

When a bond sells at a premium, a valuation account, premium on bonds payable, is credited for the amount of the premium (excess of cash proceeds over face amount). This valuation account is shown as an addition to bonds payable on the balance sheet. One of two methods can be used to amortize the premium over the life of the bonds.

1. **Straight-line method.** This method is calculated the same as it is for a discount. Premium amortization reduces interest expense for the period. The carrying value of the bonds decreases each period by the amount of bond premium amortization.
2. **Effective interest method.** The periodic bond interest expense for this method is computed in the same manner as for a bond discount. The difference between bond interest payable in cash (stated interest rate times face amount of bonds) and effective bond interest expense (effective interest rate times carrying value of bonds) is the bond premium amortization for the period.

DEFINITIONS OF KEY TERMS: LONG-TERM DEBT

Bond. A bond is a debt instrument that contains a promise to pay a specified principal amount at a determinable future date together with interest at specified times. Bonds are a good financing arrangement when relatively large sums of money are required for long periods.

Bond indenture. A bond indenture is a contract between the corporation issuing the bonds and the bondholders. It includes items such as the amount of bonds authorized, due date, interest rate, any dividend or other restrictions, and any property pledged as security.

Callable bonds. Callable bonds can be purchased from the bondholder by the issuing corporation at the issuer's option prior to maturity. If interest rates fall or an organization wishes to reduce its outstanding debt, then it may call a bond issue.

Convertible bonds. Convertible bonds allow the bondholder the option to convert the bonds into a specified number of shares of common stock.

Income bonds. Income bonds are unsecured debt where interest is paid only to the extent of an organization's current earnings. If interest is not paid due to a lack of earnings, bondholders have no claim against future earnings for the interest not paid in the current period.

Registered or coupon bonds. With registered bonds, interest is paid to the registered owner. With coupon bonds, interest is paid to the individual presenting the periodic interest coupons.

Revenue bonds. Generally, revenue bonds are issued by local governmental units, and interest and principal can be paid only from specific revenue sources.

Secured or unsecured. Secured debt has legal agreements that provide the creditor with liens on certain specified property. These liens allow creditors to sell the property pledged as security on the loan to obtain money to satisfy any unpaid balance of interest and principal.

Term or serial bonds. Term bonds occur when an entire bond issue matures on a single fixed maturity date. Serial bonds are issues that mature in installments over a period of time.

Trustee. Typically, the trustee holds the bond indenture and acts as an independent third party to protect the interests of the bond issuer and the bondholder.

The carrying value of bonds issued at a premium decreases as they mature. Therefore, the effective interest expense decreases as the bonds mature.

Any costs incurred related to the issuance of bonds, such as advertising costs, printing costs, and fees paid to underwriters, accountants, and attorneys, should be charged to a prepaid expense account. These costs should then be amortized over the life of the bond issue, because revenue results from the use of the proceeds over this period.

The reacquisition of a debt security or instrument before its scheduled maturity (except through conversion by the holder) is early extinguishment of debt. Upon early extinguishment, the bond can be formally retired or held as a treasury bond.

The net carrying amount of debt is the amount payable at maturity, adjusted for any unamortized discount, premium, or debt issue costs. The amount paid on early extinguishment, including the call premium and other reacquisition costs, is the reacquisition price of debt. *A gain on early extinguishment occurs when the net carrying amount exceeds the reacquisition price. A loss occurs when the reacquisition price exceeds the net carrying amount. A gain or loss on early extinguishment should be recognized in the period in which extinguishment occurred and reflected as a separate line item on the income statement.*

When serial bonds are sold and each maturity sells at a different yield rate, each maturity should be treated as a separate bond issue. The entire bond issue's discount or premium should be debited or credited to a single account. The amount of discount or premium amortization for each period is determined by performing a separate computation for each maturity. Either amortization method, straight-line or effective interest, may be applied to the discount or premium for each maturity. The amortization amounts for all maturities are then summarized and totaled to determine the periodic amortization.

When a note is issued solely for cash, the PV of the note is the cash proceeds. The PV of the note minus its face amount is the amount of the discount or premium. The interest expense on such a note is the stated or coupon interest plus or minus the amortization of any discount or premium.

When a note is issued in a noncash transaction and no interest rate is stated, the stated interest rate is unreasonable, or the stated face amount of the note is materially different from the current cash sales price for similar items or from the market value of the note at the date of the transaction, then the note issued and the property, goods, or services received should be recorded at the fair value of the property, goods, or services. If the fair value of the noncash item cannot be determined, then the market value of the note should be used.

A discount or premium is recognized when there is a difference between the face amount of the note and its fair value.

INTEREST RATES ON NOTES AND BONDS

The interest rate is affected by many factors, including:

- Cost of money
- Business risk factors
- Inflationary expectations associated with the business

This discount or premium should be amortized over the life of the note. If neither the fair value of the noncash item nor the market value of the note is determinable, then the PV of the note should be determined by discounting all future payments on the note using an imputed interest rate.

Short-term obligations that are expected to be refinanced on a long-term basis may be classified as long-term liabilities on the balance sheet. The requirements for classification as long-term are: Management intends to refinance the obligations on a long-term basis and demonstrates the ability to obtain the refinancing.

According to Accounting Principles Board (APB) Opinion 21, *Interest on Receivables and Payables*, **all** contractual rights to receive money or contractual obligations to pay money on fixed or determinable dates are subject to PV techniques including interest imputation.

SUGGESTED DISCLOSURES—NOTES AND BONDS

- The aggregate amount of debt net of the current portion due within one year and any discount or premium.
- Details of each debt including nature of the liability, maturity dates, interest rates, call provisions, conversion privileges, restrictive covenants, assets pledged as collateral.
- The current portion of the long-term debt is shown as a current liability unless something other than current assets will be used to satisfy the obligation.

Examples of APB opinion 21 include secured and unsecured notes, debentures, bonds, mortgage notes, equipment obligations, and some A/R and A/P. However, the following items are **exceptions**:

- Receivable and payables arising from transactions with customers or suppliers in the normal course of business that are due in customary terms not exceeding approximately one year
- Amounts that do not require repayment in the future but rather will be applied to the purchase price of the property, goods, or service involved (e.g., deposits or progress payments on construction contracts, advance payments for acquisition of resources and raw materials, advances to encourage exploration in the extractive industries)
- Amounts intended to provide security for one party to an agreement (security deposits, retainages on contracts)
- The customary cash lending activities and demand or savings deposit activities of financial institutions whose primary business is lending money
- Transactions where interest rates are affected by the tax attributes or legal restrictions prescribed by a governmental agency (e.g., industrial revenue bonds, tax-exempt obligations, government-guaranteed obligations, and income tax settlements)
- Transactions between parent and subsidiary companies and between subsidiaries of a common parent
- Warranty for product performance
- Convertible debt securities

APB Opinion 21 requires the amortization of a bond discount or premium using the **effective interest rate method**. Under this method, the total interest expense is the carrying value (book value) of the bonds at the start of the period multiplied by the effective interest rate. The objective of this method is to arrive at a periodic interest cost that will result in a constant effective rate on the carrying value of the bond at the beginning of each period. By the time the bond matures, the carrying value of the bond will be equal to the face value.

Other methods, such as the **straight-line method**, can be used if the results are not materially different. Under this method, interest expense is equal to the cash interest paid plus the amortized portion of the discount or minus the amortized portion of the premium. The amortized portion is equal to the total amount of the discount or premium divided by the life of the debt from issuance in months multiplied by the number of months the debt has been outstanding that year.

Bondholders have a prior claim to the earnings and assets of the issuing organization. They rank ahead of preferred and common stockholders. Interest must be paid to bondholders before dividends can be distributed to stockholders. Bondholders have a prior claim on assets in the case of dissolution or bankruptcy.

The following list shows the hierarchy of stakeholders.

High priority	Bondholders	• Prior claim on assets in case of dissolution or bankruptcy. • Interest must be paid first, before dividends are paid to stockholders.
	Preferred stockholders	• Prior claims on assets and dividends are paid during liquidation. • Dividends in arrears are paid.
Low priority	Common stockholders	• Low priority in case of dissolution or bankruptcy. • Receive highest benefit if the organization is successful.

(B) Extinguishment of Debt Outstanding debt may be reacquired or retired before its scheduled maturity. Usually this is caused by changes in interest rates or in cash flows. Statement of Financial Accounting Standards (SFAS) 76, *Extinguishment of Debt*, presents accounting treatment for **early** extinguishment of debt. SFAS 76 is applicable to all debt extinguishment other than debt conversions and troubled debt restructuring (the latter is addressed by SFAS 15). *Debt is now considered extinguished for financial reporting purposes in the following circumstances*:

- The debtor pays the creditor and is relieved of all of its obligations, regardless of whether the securities are canceled or held as so-called treasury bonds.
- The debtor is legally released from being the primary obligor, either judicially or by the creditor, and it is probable that the debtor will not be required to make future payments.
- The debtor irrevocably places cash or other assets in a trust to be used solely for satisfying scheduled payments of both interest and principal of a specific obligation, and the possibility that the debtor will be required to make future payments with respect to that debt is remote. In this circumstance, debt is extinguished even though the debtor is not legally released from being the primary obligor under the debt obligation.

The trust shall be restricted to owing only monetary assets that are essentially risk free as to the amount, timing, and collection of interest and principal. A monetary asset is money or a claim to receive a sum of money that is fixed or determinable without reference to future prices of specific goods or services.

SUGGESTED DISCLOSURES—EXTINGUISHMENT OF DEBT

- Aggregated gains or losses and unconditionally classified as extraordinary items
- Description of the transaction and sources of the funds used
- Income tax effect of the transaction
- Per-share amount of the aggregate gain or loss, net of tax

The monetary assets shall be denominated in the currency in which the debt is payable. For debt denominated in U.S. dollars, essentially risk-free monetary assets shall be limited to:

- Direct obligations of the U.S. government.
- Obligations guaranteed by the U.S. government.
- Securities that are backed by U.S. government obligations as collateral under an arrangement by which the interest and principal payments on the collateral generally flow immediately through to the holder of the security.

According to APB Opinion 26, *Early Extinguishment of Debt*, the difference between the net carrying value and the acquisition price is to be recorded as a gain or loss.

KEY CONCEPTS TO REMEMBER: Rules for Gains and Losses

- If the acquisition price is greater than the carrying value, a loss exists.
- If the acquisition price is less than the carrying value, a gain is generated.
- These gains or losses are to be recognized in the period in which the retirement took place.
- All gains and losses, if material in amount, should be treated as extraordinary items.
- Any gains or losses resulting from satisfying sinking fund requirements within one year are exempted from extraordinary item treatment.

(ii) Leases

A lease agreement involves at least two parties (lessor, lessee) and an asset. The lessor, who owns the asset, agrees to allow the lessee to use it for a specified period of time for rent payments. *The key point in leases is the transfer of risk of ownership.* If the transaction effectively transfers ownership to the lessee, then it should be treated as a sale even though the transaction takes the form of a lease. Here the substance, not the form, dictates the accounting treatment. Two types of leases exist: capital and operating lease.

(A) Accounting by Lessees SFAS 13, *Accounting for Leases*, requires lessees to classify every lease as either an operating lease or a capital lease. A capital lease, not an operating lease, is an installment purchase of the property.

The lessee records a capital lease as an asset and an obligation at an amount equal to the PV at the beginning of the lease term of minimum lease payments during the lease term, excluding that portion of the payments representing executory costs such as insurance, maintenance, and taxes to be paid by the lessor, together with any profit thereon.

However, if the amount so determined exceeds the fair value of the leased property at the inception of the lease, the amount recorded as the asset and obligation shall be the fair value. If the portion of the minimum lease payments representing executory costs, including profit thereon, is not determinable from the provisions of the lease, an estimate of the amount shall be made. At the inception of a capital lease, the guaranteed residual value should be included as part of minimum lease payments at PV.

SUGGESTED DISCLOSURES: LESSEE

For capital leases:

- Gross amount of assets recorded
- Future minimum lease payments in the aggregate
- Total of minimum sublease rentals to be received
- Total contingent rentals actually incurred for each period
- Depreciation

For operating leases:

- Future minimum lease payments in the aggregate
- Total of minimum rentals that will be received under noncancelable subleases
- Rental expenses separated into minimum rentals, contingent rentals, and sublease rentals

A lease meeting any one of the four criteria listed under Criterion 1 should be accounted for as a capital lease by the lessee:

Criterion 1

1. The lease transfers ownership of the property to the lessee by the end of the lease term. If the title is transferred, the lease is assumed to be a purchase and the assets should be capitalized.
2. The lease contains a bargain purchase option.
3. The lease term is equal to 75% or more of the estimated economic life of the leased property. However, if the beginning of the lease term falls within the last 25% of the total estimated economic life of the leased property, including earlier years of use, this criterion shall not be used for purposes of classifying the lease.
4. The PV at the beginning of the lease term of the minimum lease payments, excluding that portion of the payments representing executory costs such as insurance, maintenance,

and taxes to be paid by the lessor, including any profit thereon, equals or exceeds 90% of the excess of the fair value of the leased property.

Normally, rental on an operating lease shall be charged to expense over the lease term as it becomes payable. If rental payments are not made on a straight-line basis, rental expense nevertheless shall be recognized on a straight-line basis unless another systematic and rational basis is more representative of the time pattern in which use benefit is derived from the leased property, in which case that basis shall be used. *The most significant reason for choosing an operating lease over a capital lease would be to avoid an increase in the debt to equity ratio*.

(B) Accounting by Lessor From the standpoint of the lessor, if at inception a lease meets any one of the four criteria listed under Criterion 1 and in addition meets **both** of the criteria listed under Criterion 2, it shall be classified as a sales-type lease or a direct financing lease. Otherwise, it shall be classified as an operating lease.

Criterion 2

1. Collectibility of the minimum lease payments is reasonably predictable. Estimation of uncollectibility based on experience with groups of similar receivables is not a reason for applying this criterion.
2. No important uncertainties surround the amount of unreimbursable costs yet to be incurred by the lessor under the lease. The necessity of estimating executory costs, such as insurance, maintenance, and taxes to be paid by the lessor, shall not by itself constitute an important uncertainty.

SUGGESTED DISCLOSURES: LESSOR

For sales-type and direct financing leases:

- Components of the net investment in leases including future minimum lease payments, unguaranteed residual values, initial direct costs for direct financing leases, and unearned interest revenue
- Future minimum lease payments
- Total contingent rentals included in income

For operating leases:

- The cost and carrying amount of property leased
- Minimum rentals on noncancelable leases in the aggregate
- Total contingent rentals included in income

A lessor can classify a lease in four ways:

1. Sales-type leases
2. Direct financing leases
3. Operating leases
4. Participation by third parties

Sales-Type Leases The lessor should account for sales-type leases as follows:

- The minimum lease payments (net of amounts, if any, included therein with respect to executory costs such as maintenance, taxes, and insurance to be paid by the lessor, together with any profit thereon) plus the unguaranteed residual value accruing to the benefit of the lessor shall be recorded as the gross investment in the lease.
- The difference between the gross investment in the lease and the sum of the PVs of the two components of the gross investment shall be recorded as unearned income. The interest rate to be used in determining the PVs shall be the interest rate implicit in the lease. *The net investment in the lease consists of the gross investment less the unearned income.* The unearned income shall be amortized to income over the lease term so as to produce a constant periodic rate of return on the net investment in the lease. Contingent rentals, including rentals based on variables such as the prime interest rate, shall be credited to income when they become receivable.
- The PV of the minimum lease payments (net of executory costs, including any profit thereon), computed at the interest rate implicit in the lease, shall be recorded as the sales price. The cost or carrying amount, if different, of the leased property plus any initial direct costs, less the PV of the unguaranteed residual value accruing to the benefit of the lessor, computed at the interest rate implicit in the lease, shall be charged against income in the same period.
- The estimated residual value shall be reviewed at least annually. An upward adjustment of the estimated residual value should not be made while permanent reduction in the net investment should be recognized as a loss in the period in which the estimate is changed.

Direct Financing Leases The lessor should account for direct financing leases as follows:

- The minimum lease payments (as defined earlier) plus the unguaranteed residual value accruing to the benefit of the lessor should be recorded as the gross investment in the lease.

INITIAL DIRECT COST DEFINITION

Those incremental direct costs incurred by the lessor in negotiating and consummating leasing transaction including commissions and legal fees.

- The difference between the gross investment in the lease and the cost or carrying amount, if different, of the leased property shall be recorded as unearned income. The net investment in the lease should consist of the gross investment less the unearned income.

  Initial direct cost shall be charged against income as incurred, and a portion of the unearned income equal to the initial direct costs shall be recognized as income in the same period. The remaining unearned income shall be amortized to income over the lease term so as to produce a constant periodic rate of return on the net investment in the lease. Contingent rentals, including rentals based on variables such as the prime interest rate, shall be credited to income when they become receivable.
- The estimated residual value shall be reviewed at least annually and, if necessary, adjusted in the manner prescribed in sales-type leases.

Operating Leases The lessor should account for operating leases as follows:

- The leased property shall be included with or near property, plant, and equipment in the balance sheet. The property shall be depreciated following the lessor's normal depreciation policy, and in the balance sheet the accumulated depreciation shall be deducted from the investment in the leased property.
- Rent shall be reported as income over the lease term as it becomes receivable according to the provisions of the lease. However, if the rentals vary from a straight-line basis, the income shall be recognized on a straight-line basis unless another systematic and rational basis is more representative of the time pattern in which use benefit from the leased property is diminished, in which case the straight-line basis shall be used.
- Initial direct costs shall be deferred and allocated over the lease term in proportion to the recognition of rental income. However, initial direct costs may be charged to expense as incurred if the effect is not materially different from that which would have resulted from the use of the method prescribed in the preceding sentence.

Participation by Third Parties The lessor should account for participation-by-third-parties leases as follows:

- The sale or assignment of the lease or of property subject to a lease that was accounted for as a sales-type lease or direct financing lease shall not negate the original accounting treatment accorded the lease. Any profit or loss on the sale or assignment shall be recognized at the time of the transaction except that (1) when the sale or assignment is between related parties or (2) when the sale or assignment is with recourse, the profit or loss shall be deferred and recognized over the lease term in a systematic manner (e.g., in proportion to the minimum lease payments).
- The sale of property subject to an operating lease, or of property that is leased by or intended to be leased by the third-party purchaser to another party, shall not be treated as a sale if the seller or any party related to the seller retains substantial risks of ownership in the leased property.

  A seller may be by various arrangements assured recovery of the investment by the third-party purchaser in some operating lease transactions and thus retain substantial risks in connection with the property. For example, in the case of default by the lessee or termination of the lease, the arrangements may involve a formal or informal commitment by the seller to acquire the lease or the property, substitute an existing lease, or secure a replacement lessee or a buyer for the property under a remarketing agreement.
- If a sale to a third party of property subject to an operating lease or of property that is leased by or intended to be leased by the third-party purchaser to another party is not to be recorded as a sale. Instead, the transaction should be accounted for as a borrowing.

(C) Lease Involving Real Estate Lease involving real estate can be divided into four categories:

1. Leases involving land only
2. Leases involving land and buildings
3. Leases involving equipment as well as real estate
4. Leases involving only part of a building

(D) Sale-Leaseback Transaction Sale-leaseback transactions involve the sale of property by the owner and a lease of the property back to the seller. If the lease meets one of the criteria (Criterion 1) for treatment as a capital lease, the seller-lessee shall account for the lease as a capital lease; otherwise, as an operating lease.

Except as noted below, any profit or loss on the sale shall be deferred and amortized in proportion to the amortization of the leased asset, if a capital lease, or in proportion to rental payments over the period of time the asset is expected to be used, if an operating lease. However, when the fair value of the property at the time of the transaction is less than its undepreciated cost, a loss shall be recognized immediately up to the amount of the difference between undepreciated cost and fair value.

If the lease meets Criteria 1 and 2, the purchaser-lessor shall record the transaction as a purchase and a direct financing lease; otherwise, he or she shall record the transaction as a purchase and an operating lease.

(E) Accounting and Reporting for Leveraged Leases From the standpoint of the lessee, leveraged leases shall be classified and accounted for in the same manner as nonleveraged leases. The balance of this section deals with leveraged leases from the standpoint of the lessor.

A leveraged lease is defined as one having all of the following characteristics:

- It involves at least three parties: a lessee, a long-term creditor, and a lessor (commonly called the equity participant).
- Direct financing and sales-type leases are not included.

BALANCE SHEET PRESENTATION

The accounts of subsidiaries (regardless of when organized or acquired) whose principal business activity is leasing property or facilities to the parent or other affiliated companies shall be consolidated. The equity method is not adequate for fair presentation of the subsidiaries because their assets and liabilities are significant to the consolidated financial position of the enterprise.

- The financing provided by the long-term creditor is nonrecourse as to the general credit of the lessor. The amount of the financing is sufficient to provide the lessor with substantial leverage in the transaction.
- The lessor's net investment declines during the early years once the investment has been completed and rises during the later years of the lease before its final elimination. Such decrease and increase in the net investment balance may occur more than once.

The lessor shall record this investment in a leveraged lease net of the nonrecourse debt. The net of the balances of the following accounts shall represent the initial and continuing investment in leveraged leases:

- Rentals receivables, net of that portion of the rental applicable to principal and interest on the nonrecourse debt
- A receivable for the amount of investment tax credit to be realized on the transaction
- The estimated residual value of the leased asset

- Unearned and deferred income consisting of (1) the estimated pretax lease income (or loss), after deducting initial direct costs, remaining to be allocated to income over the lease term and (2) the investment tax credit remaining to be allocated to income over the lease term

The investment in leveraged leases less deferred taxes arising from difference between pretax accounting income and taxable income shall represent the lessor's net investment in leveraged leases for purposes of computing periodic net income from the lease.

For purposes of presenting the investment in a leveraged lease in the lessor's **balance sheet**, the amount of related deferred taxes shall be presented separately from the remainder of the net investment. In the **income statement** or the notes thereto, separate presentation shall be made of pretax income from the leveraged lease, the tax effect of pretax income, and the amount of investment tax credit recognized as income during the period.

KEY CONCEPTS TO REMEMBER: Leases

- A major difference between operating and financial leases is that operating leases frequently contain a cancellation clause, while financial leases are not cancelable.
- Lessee corporation has leased manufacturing equipment from lessor corporation in a transaction that is to be accounted for as a capital lease. Lessee has guaranteed lessor a residual value for the equipment. The PV of the residual guarantee should be capitalized as part of the cost of the equipment and be reflected in the financial statements of lessee.
- In accounting for a 20-year operating lease of machinery, lease expense and cash outflow would both be the same in total for the 20-year term of the lease as if the lease were capitalized.
- Rent expense is recognized for operating leases only.
- Prepaid rent is not reported for a capital lease by lessee.
- Depreciation expense is a part of items reported by a lessee for a capital lease.
- Interest expense is a part of items reported by a lessee for a capital lease.

(iii) Pensions

SFAS 87, *Employers' Accounting for Pensions*, and SFAS 88, *Employers' Accounting for Settlements and Curtailments of Defined Benefit Pension Plans and for Termination Benefits*, are the sources of GAAP in the pension area. The principal focuses of SFAS 87 are the PV of the pension obligation, the fair value of plan assets, and the disclosure of the makeup of net pension costs and of the projected benefit obligation. The critical accounting issues are the amount to be expensed on the income statement and the amount to be accrued on the balance sheet.

APPLICATION OF SFAS 87 AND 88

The scope includes unfunded, insured, trust fund, defined contribution, defined benefit plans, and deferred compensation contracts.

The scope does not include (1) independent deferred profit-sharing plans and pension payments to selected employees on a case-by-case basis; (2) plans providing only life or health insurance benefits or both; or (3) postemployment health care benefits, related assets, and obligations.

Employer commitment to employees takes the form of contributions to an independent trustee. The trustee then invests the contributions in various plan assets, such as Treasury bills and bonds, certificates of deposit (CDs), annuities, marketable securities, corporate bonds and stock. The plan assets generate interest and/or appreciate in asset value. The return on the plan assets provides the trustee the money to pay the benefits to which the employees are entitled. These benefits are defined by the terms of the pension plan using a plan's benefit formula. The formula is used to determine the pension cost for each year. The formula takes into account factors such as employee compensation, service length, age, and other factors to determine pension costs (see Exhibit 7.7).

Component	Effect
1. Service cost	Increases
2. Interest cost	Increases
3. Actual return on plan assets	Generally decreases
4. Prior service cost	Generally decreases
5. Net total of other components (gain or loss) 5 = 1 + 2 + 3 + 4	Increases or decreases

EXHIBIT 7.7 Components of Pension Expense

- Pension expense is determined by adding up five components that affect the pension expense amount, as shown in Exhibit 7.7. The service cost component is determined by the actuarial PV of benefits attributed by the pension benefit formula to employee service during that period.
- Past service cost is the portion of pension plan expense that relates to years prior to inception of the pension plan.
- The interest cost component is the interest for the period on the projected benefit obligation outstanding during the period.
- The actual return on plan assets is determined based on the fair value of plan assets at the beginning and the end of the period, adjusted for contributions and benefit payments.
- The prior service cost component is the PV of future benefits payable as a result of work done before the start of or change in a pension plan. The cost is amortized over the average remaining service period of the employees expected to receive benefits.
- Gains and losses are changes in the amount of either the projected benefit obligation or plan assets resulting from experience different from that assumed and from changes in assumptions.

(iv) Intangible Assets

Typically intangibles lack physical existence and have a high degree of uncertainty regarding their future benefits. These assets have value because of the business advantages of exclusive rights and privileges they provide. The two sources of intangible assets are listed next.

1. Exclusive privileges granted by authority of the government or legal contract, which includes patents, copyrights, trademarks, franchises, and so forth
2. Superior entrepreneurial capacity or management know-how and customer loyalty that is goodwill

Intangible assets are initially recorded at **cost**. Therefore, the costs of intangible assets, except for goodwill, are relatively easy to determine. These assets must be amortized over their expected useful life but not to exceed 40 years. An organization must use straight-line amortization, unless it can prove that another method is more appropriate. The amortization of intangible assets over their useful lives is justified by the going-concern assumption.

(A) Copyrights, Trademarks, and Patents Those intangibles that have a separate identity apart from the enterprise as a whole are identifiable as intangible assets. The most common types are listed next.

- **Copyrights.** Copyrights protect the owner from illegal reproductions of designs, writings, music, and literary productions. Purchased copyrights are recorded at cost. Research and development (R&D) costs incurred to produce a copyright internally must be expensed. The only costs that can be capitalized are the legal costs to obtain and defend the copyright. Generally, copyrights are amortized over a period of five years or less.

  A material amount of legal fees and other costs incurred by a holder of a copyright in successfully defending a copyright suit should be capitalized as part of the cost of the copyright and amortized over the remaining estimated useful life of the copyright, not to exceed 40 years. All costs should be charged to the copyright account.

SUMMARY OF AMORTIZATION PERIODS

- Copyrights not to exceed 40 years
- Trademarks not to exceed 40 years
- Patents not to exceed 17 years
- Organization costs not to exceed 40 years
- Goodwill not to exceed 40 years

- **Trademarks.** Trademarks are features such as designs, brand names, or symbols that allow easy recognition of a product. The costs to develop or acquire a trademark, except for R&D costs, are capitalized. Trademarks must be amortized over a period not to exceed 40 years.
- **Patents.** Patents are granted by the U.S. government and allow the owner exclusive benefits to a product or process over a 17-year period. Purchased patents are recorded at cost. An internally developed patent includes all costs except R&D. Legal fees incurred to successfully defend the patent should also be capitalized. A patent should be amortized over its useful life or 17 years, whichever is shorter.

TREATMENT OF R&D COSTS

R&D costs are normally expensed while organization costs, equipment costs, and goodwill costs are capitalized.

- **Organization costs.** Organization costs are incurred in the process of organizing a business. Legal fees, payments to officers for organization activities, and various state

fees may be included in organization costs. A material amount of organization costs should be amortized over five years. The period of their useful life should not exceed 40 years.

- **Franchises.** A franchise grants the right to provide a product or service or use a property. Franchise fees that are paid in advance should be capitalized and amortized over the useful life of the asset.
- **Leases.** A lease is a contract between the owner of property (lessor) and another party (lessee) that grants the right to use the property in exchange for payments. Any portion of the lease payments made in advance are capitalized in the leasehold account, an intangible asset account. Another intangible account, leasehold improvements, is established for any improvements to the leased property by the lessee. Leasehold improvements should be amortized over their useful life or the remaining life of the lease, whichever is shorter. The leasehold is amortized over the life of the lease.

(B) Goodwill Some intangible assets, since they cannot be separated from the business as a whole, are not specifically identifiable. Goodwill is a prime example of this type of intangible.

Goodwill arises when an organization's value as a whole exceeds the fair market value of its net assets. This typically occurs when an organization generates more income than other organizations with the same assets and capital structure. Superior management, a superior reputation, and a valuable customer list are factors that may contribute to these excess earnings.

SUGGESTED DISCLOSURES FOR INTANGIBLE ASSETS

- Description of the nature of the assets
- Amount of amortization expense for the period and the method used
- Amortization period used
- Amount of accumulated amortization

Goodwill is something that develops over time through the generation of these excess earnings. However, since no objective measure of the total value of a business is available until it is sold, goodwill is not recorded unless a business is purchased.

To calculate goodwill, a portion of the total cost of the acquired organization should be allocated to the tangible and intangible assets based on their fair market values. Goodwill is the difference between the cost allocated to these assets and the total cost of the acquisition.

The amortization period for goodwill arising after October 31, 1970, should not exceed 40 years. Goodwill before October 31, 1970, does not have to be amortized until the useful life of the goodwill becomes known.

Negative goodwill is created when the fair market value of the acquired net assets exceeds the cost of the acquired company. This excess is allocated proportionately to reduce noncurrent assets

except for long-term investments in marketable securities. If noncurrent assets are reduced to zero, then the excess should be recorded as a deferred credit and amortized over a period not to exceed 40 years.

Estimating the value of goodwill prior to the consummation of a purchase requires estimating future expected excess earnings and calculating their PV. The same result should be achieved by determining the PV of the total expected future earnings of the organization, which is the total value of the firm. The total value of the firm minus the value of the identifiable tangible and intangible net assets is estimated goodwill.

RULES FOR GOODWILL

- If goodwill is internally generated, expense it.
- If goodwill is purchased, capitalize it.

(v) Research and Development

(A) R&D Costs SFAS 2, *Accounting for Research and Development (R&D) Costs*, requires R&D costs to be expensed as incurred except for intangible or fixed assets purchased from others having alternative future uses. Thus, the cost of patents and R&D equipment purchased from third parties may be deferred, capitalized, and amortized over the assets' useful life. However, internally developed R&D may not be deferred and therefore should be expensed. R&D done under contract for others is not required to be expensed per SFAS 2. The costs incurred would be matched with revenue using the completed-contract or percentage-of-completion method. The key accounting concept is expense R&D costs as incurred and disclose total R&D expenses per period on the face of income statement or notes.

Under R&D activities, the *Standard* includes laboratory research to discover new knowledge, formulation, and design of product alternatives (e.g., testing and modifications); preproduction prototypes and models (e.g., tools, dies, and pilot plants); and engineering activity until product is ready for manufacture.

The *Standard* excludes these nine R&D activities:

1. Engineering during an early phase of commercial production
2. Quality control for commercial production
3. Troubleshooting during commercial production breakdowns
4. Routine, ongoing efforts to improve products
5. Adaptation of existing capability for a specific customer
6. Seasonal design changes to products
7. Routine design of tools and dies
8. Design, construction, and start-up of equipment except that used solely for R&D
9. Legal work for patents or litigation

Item 9 is capitalized while all the other eight items are expensed.

Elements of R&D costs are listed next.

- Materials, equipment, and facilities
- Salaries, wages, and related costs
- Intangibles purchased from others are treated as materials
- R&D services performed by others
- Reasonable allocation of indirect costs, excluding general and administrative costs not clearly related to R&D.

(B) Software Developed for Sale or Lease The costs that are incurred internally to create the software should be expensed as R&D costs until technological feasibility is established. Thereafter, all costs should be capitalized and reported at the lower of unamortized cost or net realizable value. Capitalization should cease when the software is available for general release to customers.

The annual amortization of capitalized computer software costs will be the greater of the ratio of current revenues to anticipated total revenues or the straight-line amortization that is based on the estimated economic life. Once the software is available for general release to customers, the inventory costs should include costs for duplicating software and for physically packaging the product. The cost of maintenance and customer support should be charged to expense in the period incurred.

(C) Software Developed for Internal Use Software must meet two criteria to be accounted for as internally developed software:

1. The software's specifications must be designed or modified to meet the reporting entity's internal needs, including costs to customize purchased software.
2. During the period in which the software is being developed, there can be no plan or intent to market the software externally, although development of the software can be jointly funded by several entities that each plan to use the software internally.

In order to justify capitalization of related costs, it is necessary for management to conclude that it is probable that the project will be completed and that the software will be used as intended. Absent that level of expectation, costs must be expensed currently as R&D costs are required to be. Entities that historically were engaged in both R&D of software for internal use and for sale to others would have to carefully identify costs with one or the other activity, since the former would be subject to capitalization while the latter might be expensed as R&D costs until technological feasibility had been demonstrated.

Under terms of the *Standard*, cost capitalization commences when an entity has completed the conceptual formulation, design, and testing of possible project alternatives, including the process of vendor selection for purchased software, if any. These early-phase costs (i.e., preliminary project stage costs) are similar to R&D costs and must be expensed as incurred.

Costs incurred subsequent to the preliminary project stage, and that meet the criteria under GAAP as long-lived assets, can be capitalized and amortized over the asset's expected economic life. Capitalization of costs will begin when both of two conditions are met.

1. Management having the relevant authority approves and commits to funding the project and believes that it is probable that it will be completed and that the resulting software will be used as intended.
2. The conceptual formulation, design, and testing of possible software project alternatives (i.e., the preliminary project stage) have been completed.

(c) Advanced Concepts of Financial Accounting

In this section, business combination, consolidation, partnerships, and foreign currency transactions are discussed.

(i) Business Combination

(A) Overview According to FASB, a business combination occurs when an entity acquires net assets that constitute a business or acquires equity interests of one or more other entities and obtains control over that entity or entities. Business combinations may be friendly or hostile takeovers. Purchase accounting is the only acceptable accounting method for all business combinations; the pooling-of-interest method is not.

FASB Statement 141 identified these key components of the purchase method of accounting:

- **Initial recognition.** Assets are commonly acquired in exchange transactions that trigger the initial recognition of the assets acquired and any liabilities assumed.
- **Initial measurement.** Like other exchange transactions generally, acquisitions are measured on the basis of the fair values exchanged.
- **Allocating costs.** Acquiring assets in groups requires not only ascertaining the cost of the assets (or net assets) group but also allocating that cost to the individual assets (or individual assets and liabilities) that make up the group.
- **Accounting after acquisition.** The nature of an asset and not the manner of its acquisitions determines an acquiring entity's subsequent accounting for the asset.

According to the FASB, the **combinor** is a constituent company entering into a purchase-type business combination whose stockholders as a group retain or receive the largest portion of the voting rights and control over the combined enterprise and thereby can elect a majority of the governing board of directors or other group of the combined enterprise. The **combinee** is a constituent company other than the combinor involved in a business combination.

(B) Computation and Allocation of Cost of a Combinee The cost of a combinee is the total of the amount of consideration paid by the combinor, the combinor's direct out-of-pocket costs of the combination, and any contingent consideration that is determinable on the date of the business combination.

The amount of consideration is the total amount of cash paid, the current fair value of other assets distributed, the PV of debt securities issued, and the current fair value (or market) value of equity securities issued by the combinor.

The direct out-of-pocket costs include some legal fees, some accounting fees, and finder's fees (paid to investment banking firm). Costs of registering with the Securities and Exchange Commission

(SEC) and issuing debt securities are not part of the direct cost of the combinee. Costs of registering with the SEC and issuing equity securities are not part of direct costs either but can be offset against the proceeds from the issuance of the equity securities.

Contingent consideration is additional cash, other assets, or securities that may be issuable in the future, contingent on future events such as a specified level of earnings or a designated market price for a security that had been issued to complete the business combination. Contingent consideration can be determinable or not determinable for recording as part of the cost of the combination.

The FASB requires that the cost of a combinee must be allocated to assets (other than goodwill) acquired and liabilities assumed based on their estimated fair values on the date of the combination. Any excess of total costs over the amounts thus allocated is assigned to goodwill. Methods for determining fair values are listed next.

- PVs for receivables and most liabilities
- Net realizable value less a reasonable profit for work in process (WIP) and finished goods inventories
- Appraised values for land, natural resources, and nonmarketable securities
- Individual fair values for patents, copyrights, franchises, customer lists, and unpatented technology

(ii) Consolidation

The purpose of consolidated financial statements is to present for a single accounting entity the combined resources, obligations, and operating results of a group of related corporations, such as parent and subsidiaries. Only subsidiaries not actually controlled should be exempted from consolidation. Usually an investor's direct or indirect ownership of more than 50% of an investee's outstanding common stock has been required to evidence the controlling interest underlying a parent–subsidiary relationship. Actual control is more important than the controlling interest in situations such as liquidation or reorganization (bankruptcy) of a subsidiary or control of a foreign subsidiary by a foreign government. GAAP requires the use of the cost method of accounting for investments in unconsolidated subsidiaries because the subsidiaries generally are neither controlled nor significantly influenced by the parent company.

Assets, liabilities, revenues, and expenses of the parent company and its subsidiaries are totaled; intercompany transactions and balances are eliminated; and the final consolidated amounts are reported in the consolidated balance sheet, income statement, statement of stockholders' equity, statement of retained earnings, and statement of cash flows.

(A) Consolidation of Wholly Owned Subsidiary Using Purchase Accounting Method (on Date of Purchase Combination) The parent company's investment account and the subsidiary's stockholders' equity accounts do not appear in the consolidated balance sheet because they are intercompany (reciprocal) accounts. Under purchase accounting theory, the parent company assets and liabilities (except intercompany) are reflected at carrying amounts, and the subsidiary assets and liabilities (except intercompany) are reflected at current fair values, in the consolidated balance sheet. Goodwill is recognized to the extent the cost of the parent's investment in 100% (wholly owned)

of the subsidiary's outstanding common stock exceeds the current fair value of the subsidiary's identifiable net assets.

(B) Consolidation of Partially Owned Subsidiary Using Purchase Accounting Method (on Date of Purchase Combination) The recognition of minority interest is handled differently between the wholly owned subsidiary and the partially owned subsidiary. Minority or noncontrolling interest refers to the claims of stockholders other than the parent company to the net income or losses and net assets of the subsidiary. The minority interest in the subsidiary's net income or losses is displayed in the consolidated income statement, and the minority interest in the subsidiary's net assets is displayed in the consolidated balance sheet.

Minority interest is accounted for in two ways: the parent company concept, which emphasizes the interests of the parent's shareholders, and the economic unit concept, which emphasizes the legal aspect and the entity theory. The parent company concept treats the minority interest in net assets of a subsidiary as a liability. This liability is increased each accounting period subsequent to the date of a purchase-type business combination by an expense representing the minority's share of the subsidiary's net income or decreased by the minority's share of the subsidiary's net loss. Dividends declared by the subsidiary to minority stockholders decrease the liability to them. Consolidated net income is net of the minority's share of the subsidiary's net income. In the economic unit concept, the minority interest in the subsidiary's net assets is displayed in the stockholders' equity section of the consolidated balance sheet. The consolidated income statement displays the minority interest in the subsidiary's net income as a subdivision of total consolidated net income, similar to the distribution of net income of a partnership.

(C) Consolidation of Wholly Owned Subsidiary Using Purchase Accounting Method (Subsequent to Date of Purchase Combination) Subsequent to the date of a business combination, the parent company must account for the operating results of the subsidiary: the net income or net loss and dividends declared are paid by the subsidiary. In addition, a number of intercompany transactions and events that occur in a parent–subsidiary relationship must be recorded.

In accounting for the operating results of consolidated purchased subsidiaries, a parent company may choose the equity method or the cost method of accounting. In the equity method, the parent company recognizes its share of the subsidiary's net income or net loss, adjusted for depreciation and amortization of differences between current fair values and carrying amounts of a purchased subsidiary's net assets on the date of the business combination, as well as its share of dividends declared by the subsidiary. In the cost method, the parent company accounts for the operations of a subsidiary only to the extent that dividends are declared by the subsidiary. Dividends declared by the subsidiary from net income subsequent to the business combination are recognized as revenue by the parent company; dividends declared by the subsidiary in excess of postcombination net income constitute a reduction of the carrying amount of the parent company's investment in the subsidiary. Net income or net loss of the subsidiary is not recognized by the parent company when using the cost method.

The equity method is consistent with the accrual basis of accounting and stresses the economic substance of the parent–subsidiary relationship due to single economic entity concept. The equity method is appropriate for pooled subsidiaries as well as purchased subsidiaries. The cost method recognizes the legal form of the parent–subsidiary relationship. The

cost method is compatible with purchase accounting only, and there is no cost to pooled subsidiary. Consolidated financial statement amounts are the same, regardless of whether a parent company uses the equity method or the cost method to account for a subsidiary's operations.

(D) Consolidation of Partially Owned Subsidiary Using Purchase Accounting Method (Subsequent to Date of Purchase Combination Accounting for the operating results of a partially owned subsidiary requires the computation of the minority interest in net income or net losses of the subsidiary. Thus, under the parent company concept of consolidated financial statements, the consolidated income statement of a parent company and its partially owned purchased subsidiary includes an expense—minority interest in net income (or loss) of subsidiary. The minority interest in net assets of the subsidiary is displayed among liabilities in the consolidated balance sheet.

(E) Accounting for Intercompany Transactions Not Involving Profit (Gain) or Loss Subsequent to the date of a business combination, a parent company and its subsidiaries may enter into a number of transactions with each other. Both the parent and the subsidiary should account for these intercompany transactions in a manner that facilitates the consolidation process. Separate ledger accounts should be established for all intercompany assets, liabilities, revenues, and expenses. These separate accounts clearly identify the intercompany items that must be eliminated in the preparation of consolidated financial statements. After elimination, the consolidated financial statements include only those balances and transactions resulting from outside entities.

(F) Accounting for Intercompany Transactions Involving Profit (Gain) or Loss Many business transactions between a parent company and its subsidiaries involve a profit (gain) or loss. Among these transactions are intercompany sales of merchandise, intercompany sales of plant assets, intercompany leases of property under capital lease or sales-type lease, and intercompany sales of intangible assets. Until intercompany profits or losses in such transactions are realized through the sales of the asset to an outsider or otherwise, the profits or losses must be eliminated in the preparation of consolidated financial statements.

In addition, a parent or subsidiary company's acquisition of its affiliate's bonds in the open market may result in a realized gain or loss to the consolidated entity. Such a realized gain or loss is not recognized in the separate income statement of either the parent company or the subsidiary, but it must be recognized in the consolidated income statement.

(iii) Partnerships

A partnership is an association of two or more people to carry on as co-owners of a business for profit. Competent parties agree to place their money, property, or labor in a business and to divide the profits and losses. Each person is personally liable for the debts of the partnership. Express partnership agreements may be oral or written.

Partnerships are not subject to the income tax. The partnership net profit or loss is allocated to each partner according to the partnership's profit-sharing agreement. Each partner reports these items on his or her own tax return. Several separately reported items (e.g., capital gains, charitable contributions) retain their character when passed through to the partners.

DEFINITIONS OF KEY TERMS: PARTNERSHIPS

Dormant partner. A partner who is both silent and secret

General partner. A partner who is liable for all partnership liabilities plus any unpaid contributions

Limited partner. A partner who is obligated to the partnership to make any contribution stated in the certificate, even if he or she is unable to perform because of death, disability, or any other reason

Secret partner. A partner who may advise management and participate in decisions, but his interest is not known to third parties

Silent partner. A partner who does not participate in management

(A) Duties, Rights, and Powers of Partners The duties, rights, and powers of partners are both expressed (in the agreement) and implied (created by law). In most states, the statutory law is the Uniform Partnership Act.

All partners have equal rights in management and conduct of business, even if their capital contributions are not equal. The partners may agree to place management within the control of one or more partners.

Ordinary matters are decided by a majority of the partners. If the partnership consists of two persons who are unable to agree and the partnership agreement makes no provision for arbitration, then dissolution is the only remedy.

The following matters require the unanimous consent of the partners:

- Change the essential nature of the business by altering the original agreement or reducing or increasing the partners' capital
- Embark on a new business or admit new members
- Modify a limited partnership agreement
- Assign partnership property to a trustee for the benefit of creditors
- Confess a judgment
- Dispose of the partnership's goodwill
- Submit a partnership agreement to arbitration
- Perform an act that would make impossible the conduct of the partnership business

However, the process of "engaging a new client" does not require unanimous consent of the partners.

Partners are not entitled to payment for services rendered in conducting partnership business, but they may receive a salary. The payment of a salary to a partner requires either an express agreement stating such or may be implied from the partner's conduct.

Capital contributions are not entitled to draw interest; a partner's earnings on his or her capital investment are his or her share of the profits. Interest may be paid on advances to the partnership

above the amount of original contributed capital. Profits that are not withdrawn but left in the partnership are not entitled to draw interest.

Each partner has the duty to give the person responsible for record keeping any information necessary to efficiently and effectively carry on business. Each partner has the right to inspect the records at any time, but no partner can remove the records from the agreed-on location without the other partners' consent. Copies of the records can be made.

Knowledge known to one partner and not revealed to the other partners is considered notice to the partnership. A partner should communicate known facts to the other partners and have them added to the partnership records. *A partner who possesses knowledge and does not reveal it to the other partners has committed an act of fraud.*

Every partner has an equal right to possess partnership property for partnership purposes. Possession of partnership property for other purposes requires the other partners' permission. A partner cannot transfer partnership property or use partnership property in satisfaction of personal debts.

In the case of a partner's death, his or her interest in specific partnership property passes to the surviving partners. The surviving partners wind up the affairs of the partnership in accordance with the partnership agreement and the applicable laws.

Partners owe each other the duty of undivided loyalty, since a partnership is a fiduciary relationship. Each partner must exercise good faith and consider the mutual welfare of all the partners in conducting business.

Partners have the following powers.

- **Power to contract.** The general laws of agency apply to partnerships, since a partner is considered an agent for the partnership business. A partner may bind the partnership with contractual liability whenever he is apparently carrying on the partnership business in the usual manner. Otherwise, a partner cannot bind the partnership without the authorization of the other partners.
- The **common implied powers** of a partner include the ability to
  - Compromise, adjust, and settle claims or debts owed by or to the partnership.; Sell goods in the regular course of business and make warranties.;
  - Buy property within the scope of the business for cash or on credit.
  - Buy insurance.
  - Hire employees.
  - Make admissions against interest.
  - Enter into contracts within the scope of the firm.
  - Receive notices.
- **Power to impose tort liability.** The law imposes tort liability on a partnership for all wrongful acts or omissions of any partner acting in the ordinary course of the partnership and for its benefit. The partnership has the right of indemnity against the partner at fault.
- **Power over property.** Partners have implied authority to sell to good-faith purchasers personal property that is held for resale and to execute the necessary documents to transfer

title. Selling the fixtures and equipment used in the business requires the other partners' authorization.

The right to sell a business's real property is implied only if it is in the real estate business. Other transfers of real property require partnership authorization.

- **Financial transactions.** Partnerships are divided into general classes, trading and nontrading partnerships, to determine the limit of a partner's financial powers. A **trading partnership** engages in the business of buying and selling merchandise. Each partner has an implied power to borrow money and to extend the credit of the firm, in the usual course of business, by signing negotiable paper.

  A **nontrading partnership** engages in the production of merchandise or sells services. In these partnerships, a partner's powers are more limited. A partner does not have the implied power to borrow money.

(B) Liabilities and Authorities of a General Partner General partners are liable for:

- Fraudulent acts of other partners.
- Debts attributable to limited partner notes to the partnership.
- Debts related to the purchase of real property without each partner's consent.

General partners have no authority to:

- Do any act in violation of the certificate.
- Do any act that would make it impossible to carry on the ordinary business of the partnership.
- Confess a judgment against the partnership.
- Possess or assign partnership property for other than partnership purposes.
- Admit a person as a general partner.
- Admit a person as a limited partner unless the right to do so is given in the certificate.
- Continue the business with partnership property on the death, retirement, or incapacity of a general partner unless the right to do so is given in the certificate.

(C) Partnership Accounting A partner's share of the partnership assets or profits may be determined in a suit for an accounting. These suits are equitable in nature and must be filed in a court of equity. A partner is entitled to a formal accounting in the following situations:

- The partnership has been dissolved.
- An agreement calls for an accounting at a definite date.
- A partner has withheld profits arising from secret transactions.
- An execution has been levied against the interest of one of the partners.
- One partner does not have access to the books.
- The partnership is approaching insolvency, and all parties are not available.

Partners may make a complete accounting and settle their claims without resort to a court of equity. An accounting is performed on the dissolution of a solvent partnership and winding up of its business. All firm creditors other than partners are entitled to be paid before the partners are entitled to participate in any of the assets.

The assets are distributed among the partners in these ways:

- Any partner who has made advances to the firm or has incurred liability for, or on behalf of, the firm is entitled to reimbursement.
- Each partner is entitled to return of his or her capital contributions.
- Any remaining balance is distributed as profits in accordance with the partnership agreement.

(D) Actions Against Other Partners Typically a partner cannot maintain an action at law against the other partners, because the indebtedness among the partners is undetermined until there is an accounting and all partnership affairs are settled. *The three exceptions to this rule are if*

1. The partnership is formed to carry out a single venture or transaction;
2. The action involves a segregated or single unadjusted item or account; or
3. The action involves a personal covenant or transaction entirely independent of the partnership affairs.

(E) Admitting a New Partner If a partnership admits a new partner, the new partner is liable to the extent of his capital contribution for all obligations incurred before his admission. The new partner is not personally liable for such obligations.

(F) Asset Distribution of Partnership If a firm is insolvent and a court of equity is responsible for the distribution of the partnership assets, the assets are distributed in accordance with a rule known as **marshalling of assets**. The firm's creditors may seek payment out of the firm's assets and then the individual partner assets. The firm's creditors must exhaust the firm's assets before recourse to the partners' individual assets. *The descending order of asset distribution of a limited partnership is listed next.*

1. Secured creditors other than partners
2. Unsecured creditors other than partners
3. Limited partners in respect of their profits
4. Limited partners in respect of their capital contributions
5. General partners in respect of any loans to the partnership
6. General partners in respect of their profits
7. General partners in respect of their capital contributions

The **asset distribution hierarchy** of a limited partnership is shown in Exhibit 7.8.

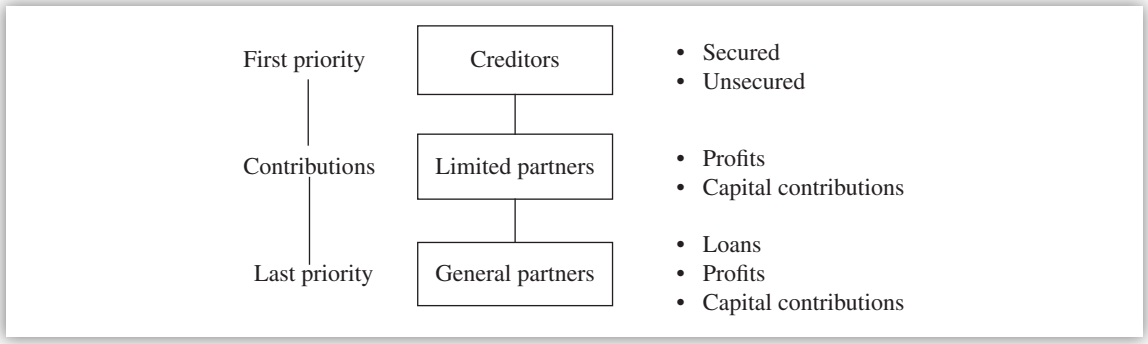


EXHIBIT 7.8 Asset Distribution Hierarchy

(iv) Foreign Currency Transactions

The buying and selling of foreign currencies result in variations in the exchange rate between the currencies of two countries. The bank's selling spot rate is what it charges for current sales of the foreign currency. The bank's buying spot rate for the currency is less than the selling spot rate; the spread between the selling and buying spot rates represents gross profit to a trader in foreign currency. Factors influencing fluctuations in exchange rates include: a nation's balance of payments surplus or deficit; differing global rates of inflation; and money market variations, such as interest rates, capital investment levels, and monetary policies and actions of central banks.

A multinational corporation (MNC) headquartered in the United States engages in sales, purchases, and loans with foreign companies as well as with its own branches, divisions, investees, and subsidiaries in other countries. If the transactions with foreign companies are denominated in terms of the U.S. dollar, no accounting problems arise for the U.S.-based MNC. If the transactions are negotiated and settled in terms of the foreign companies' local currency unit, then the U.S. company must account for the transaction denominated in foreign currency in terms of U.S. dollars. This foreign currency translation is accomplished by applying the appropriate exchange rate between the foreign currency and the U.S. dollar.

In addition to spot rates, forward rates apply to foreign currency transactions to be completed on a future date. Forward rates apply to forward exchange contracts, which are agreements to exchange currencies of different countries on a specified future date at the forward rate in effect when the contract was made. Forward rates may be larger or smaller than spot rates for a foreign currency, depending on the foreign currency dealer's expectations regarding fluctuations in exchange rates for the currency.

Increases in the selling spot rate for a foreign currency required by a U.S.-based MNC to settle a liability denominated in that currency generate transaction losses to the company because more dollars are required to obtain the foreign currency. Conversely, decreases in the selling spot rate produce transaction gains to the company because fewer U.S. dollars are required to obtain the foreign currency. In contrast, increases in the buying spot rate for a foreign currency to be received by a U.S.-based MNC in settlement of a receivable denominated in that currency generate transaction gains to the company; decreases in the buying spot rate produce transaction losses.

(A) Translation of Foreign Currency Financial Statements When a U.S.-based MNC prepares consolidated or combined financial statements that include the operating results, financial position (balance sheet), and cash flows of foreign subsidiaries or branches, the U.S. company must translate the amounts in the final statements of the foreign entities from the entities' functional currency to U.S. dollar. Similar treatment must be given to investments in other foreign investees for which the U.S. company uses the equity method of accounting.

Four methods are available to translate foreign currency: current/noncurrent, monetary/nonmonetary, current rate, and temporal method. The temporal method is the same as the monetary/nonmonetary method.

Current/Noncurrent Method Current assets and current liabilities are translated at the exchange rate in effect on the balance sheet date of the foreign entity (i.e., the current rate). All other assets and liabilities, and the components of owners' equity, are translated at the historical rates in effect at the time the assets, liabilities, and equities first were recognized in the foreign entity's accounting records. In the income statement, depreciation expense and amortization expense are

translated at historical rates applicable to the related assets, while all other revenue and expenses are translated at an average exchange rate for the accounting period.

This method reflects the liquidity aspects of the foreign entity's financial position by showing the current U.S. dollar equivalents of its working capital components. Inventories are translated at the current rate, which is a departure of the historical rate.

Monetary/Nonmonetary Method Monetary assets and liabilities, which are expressed in a fixed amount, are translated at the current exchange rate. All other assets, liabilities, and owners' equity amounts are translated at appropriate historical rates. In the income statement, average exchange rates are applied to all revenue and expenses except depreciation expense, amortization expense, and COGS, which are translated at appropriate historical rates.

This method emphasizes the retention of the historical-cost principle in the foreign entity's financial statements and parent company aspects of a foreign entity's financial position and operating results. Due to use of the parent company's reporting currency, this method misstates the actual financial position and operating results of the foreign entity.

Current Rate Method All balance sheet accounts other than owners' equity are translated at the current exchange rate. Owners' equity amounts are translated at historical rates. To emphasize the functional currency aspects of the foreign entity's operations, all revenue and expenses may be translated at the current rate on the respective transaction dates, if practical. Otherwise, an average exchange rate is used for all revenue and expenses.

(B) Transaction Gains and Losses Excluded from Net Income Gains and losses from the following foreign currency transactions should be accounted for in the same manner as translation adjustments:

- Foreign currency transactions that are designated, and are effective, as economic hedges of a net investment in a foreign entity, commencing as of the designation date
- Intercompany foreign currency transactions that are of a long-term investment nature, when the entities to the transaction are consolidated, combined, or accounted for by the equity method

(C) Functional Currency in Highly Inflationary Economies The functional currency of a foreign entity in a highly inflationary economy can be identified as the reporting currency (e.g., the U.S. dollar for a U.S.-based MNC). A highly inflationary economy is defined as the one having cumulative inflation of 100% or more over a three-year period. The financial statements of a foreign entity in a country experiencing severe inflation are remeasured in U.S. dollars.

(D) Income Taxes Related to Foreign Currency Translation The procedures for the interperiod and intraperiod tax allocation to determine the effects of foreign currency translation are listed next.

- Interperiod tax allocation for temporary differences associated with transaction gains and losses are reported in different accounting periods for FA and income taxes.
- Interperiod tax allocation for temporary differences associated with translation adjustments that do not meet the criteria for nonrecognition of deferred tax liabilities for undistributed earnings of foreign subsidiaries.

- Intraperiod tax allocation for translation adjustments are included in the stockholders' equity section of the balance sheet.

(E) Disclosure of Foreign Currency Translation Aggregate transaction gains or losses of an accounting period should be disclosed in the income statement or in a note to the financial statements. Changes in cumulative translation adjustments during an accounting period should be disclosed in a separate financial statement, in a note to financial statements, or in a statement of stockholders' equity.

The minimum required disclosures include:

- Beginning and ending amounts of cumulative translation adjustments.
- Aggregate adjustments during the accounting period for translation adjustments, hedges of net investments, and long-term intercompany transactions.
- Income taxes allocated to translation adjustments during an accounting period.
- Decreases resulting from sale or liquidation of an investment in a foreign entity.

(d) Financial Statement Analysis

(i) Overview

Financial statement analysis requires a comparison of the firm's performance with that of other firms in the same industry, with its own previous performance, and/or both. Three major parties who analyze financial statements from their own perspectives are: (1) managers of the firm to gauge performance, (2) potential investors who want to invest in the firm by purchasing stocks and bonds, and (3) creditors and lenders (e.g., bankers) who analyze data in financial statements to assess the financial strength of the firm and its ability to pay interest and principal for the money they lent to the firm. Investors use data in financial statements to form expectations about future earnings and dividends and to determine the riskiness of these expected values. *The real value of financial statements is in their predictive power about the firm's future earnings potential and dividends payment strength.*

WHO LOOKS FOR WHAT?

- Investors look for earnings and dividends, and this is reflected in security values. Therefore, cash flows are the major basis for security values.
- Creditors look for asset strength and the ability to pay off the debt.
- Financial statements report accounting profits.
- High accounting profits generally mean high cash flows and the ability to pay high dividends and debt payments.

A company's **annual report** presents four basic financial statements, including: a statement of income (income statement), a statement of financial position (balance sheet), a statement of retained earnings, and a statement of cash flows. The income statement summarizes the firm's revenues and expenses over an accounting period.

An **income statement** presents the results of operations for a given time period. Net sales are shown at the top; then various costs, including income taxes, are subtracted to obtain the net income available to common stockholders. A report on earnings and dividends per share is given at the bottom of the statement.

A **balance sheet** is a statement of the firm's financial position at a specific point in time. The firm's assets are shown on the left-hand side of the balance sheet while liabilities and equity (the claims against these assets) are shown on the right-hand side. The assets are listed in the order of their liquidity or the length of time it takes to convert assets into cash. The liabilities are listed in the order in which they must be paid.

A **statement of retained earnings** shows how much of the firm's earnings were not paid out in dividends. Retained earnings represent a claim against assets, not assets per se. Retained earnings do not represent cash and are not "available" for the payment of dividends or anything else. A positive retained earnings means that the firm has earned an income, but its dividends have been less than its reported income. Due to differences between accrual and cash accounting practices, a firm may earn money, which shows an increase in the retained earnings, but still be short of cash.

A **statement of cash flows** reports the impact of a firm's operating, investing, and financing activities on cash flows over an accounting period. This statement shows how the firm's operations have affected its cash flows and presents the relationships among cash flows from operating, investing, and financing activities of the firm.

(ii) Types of Financial Statement Analysis

Four types of measures that are used to analyze a company's financial statements and its financial position include common size analysis, trend analysis, comparative ratios, and single ratios (see Exhibit 7.9).

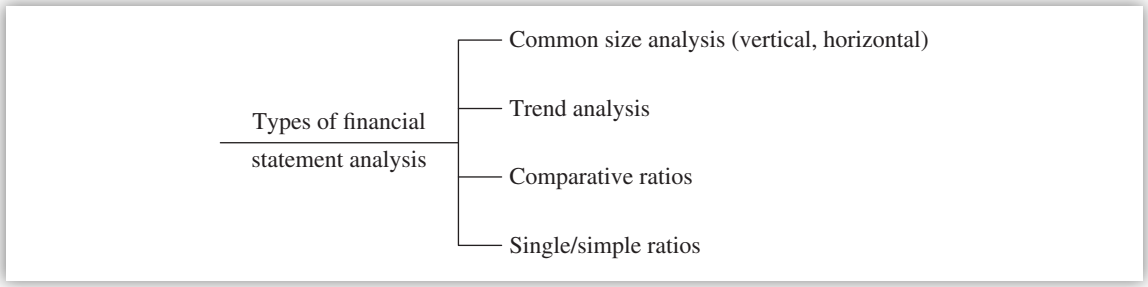


EXHIBIT 7.9 Types of Financial Statement Analysis

Common size analysis expresses items in percentages, which can be compared with similar items of other firms or with those of the same firm over time. For example, common size balance sheet line items (both assets and liabilities) are expressed as a percentage of total assets (e.g., receivables as X% of total assets). Similarly, common size income statement line items are expressed as a percentage of total sales (e.g., COGS as X% of total sales).

Variations of common size analysis include vertical analysis and horizontal analysis. **Vertical analysis** expresses all items on a financial statement as a percentage of some base figure, such as total assets or total sales. Comparing these relationships between competing organizations helps to isolate strengths and areas of concern.

In **horizontal analysis**, the financial statements for two years are shown together with additional columns showing dollar differences and percentage changes. Thus, the direction, absolute amount, and relative amount of change in account balances can be calculated. Trends that are difficult to isolate through examining the financial statements of individual years or comparing with competitors can be identified.

Trend analysis shows trends in ratios, which gives insight as to whether the financial situation of a firm is improving, declining, or stable. It shows a graph of ratios over time, which can be compared with a firm's own performance as well as that of its industry.

Comparative ratios show key financial ratios, such as current ratio and net sales to inventory, by industry, such as beverages and bakery products. These ratios represent average financial ratios for all firms within an industry category. Many organizations that supply ratio data exist; each designs ratios for its own purpose, such as small firms or large firms. Also, the focus of these ratios is different, such as creditors' viewpoint or investors' viewpoint. Another characteristic of organization that supply ratio data is that each has its own definitions of the ratios and their components. Due to these differences, a caution is required when interpreting these ratios.

Another type of comparative analysis is comparing the financial statements for the current year with those of the most recent year. By comparing summaries of financial statements for the last five to ten years, an individual can identify trends in operations, capital structure, and the composition of assets. This comparative analysis provides insight into the normal or expected account balance or ratio, information about the direction of changes in ratios and account balances, and insight into the variability or fluctuation in an organization's assets or operations.

TREND ANALYSIS VERSUS COMPARATIVE RATIO ANALYSIS

- In trend analysis, trends are shown over time between the firm and its industry.
- In comparative ratio analysis, a single point (one-to-one) comparison is shown between the firm and its industry.
- In both analyses, the industry's ratio is an average ratio, while the firm's ratio is not.

Next, our major focus shifts to **single ratios or simple ratios**. Certain accounts or items in an organization's financial statements have logical relationships with each other. If the dollar amounts of these related accounts or items are expressed in fraction form, they are called ratios. These ratios are grouped into five categories:

1. Liquidity ratios
2. Asset management ratios
3. Debt management ratios
4. Profitability ratios
5. Market value ratios

Exhibit 7.10 presents individual ratios for each ratio category.

(iii) Single/Simple Ratios

Details on liquidity ratios, asset management ratios, debt management ratios, profitability ratios, and market value ratios are presented next.

(A) Liquidity Ratios Liquidity ratios measure an organization's debt-paying ability, especially in the short term. Examples include current ratio, quick ratio, and free cash flows. These ratios indicate

Ratio category	Individual ratios
Liquidity (1)	Current ratio, quick ratio or acid-test ratio
Asset management (2)	Inventory turnover ratio, days sales outstanding ratio, fixed assets turnover ratio, total assets turnover ratio
Debt management (3)	Debt to total assets ratio, times-interest-earned ratio, fixed charge coverage ratio, cash flow coverage ratio
Profitability (4) = (1) + (2) + (3)	Profit margin on sales ratio, basic earning power ratio, return on total assets ratio, return on common equity ratio, earnings per share ratio, payout ratio
Market value (5) = (1) + (2) + (3) + (4)	Price/earnings ratio, book value per share ratio, market/book ratio

EXHIBIT 7.10 Individual Financial Ratios

an organization's capacity to meet maturing current liabilities and its ability to generate cash to pay these liabilities.

Current Ratio (Working Capital Ratio): Current Assets Divided by Current Liabilities Current ratios indicate an organization's ability to pay its current liabilities with its current assets and, therefore, show the strength of its working capital position. A high current ratio indicates a strong liquidity and vice versa. While a high current ratio is good, it could also mean excessive cash, which is not good.

Both short-term and long-term creditors are interested in the current ratio, because a firm unable to meet its short-term obligations may be forced into bankruptcy. Many bond indentures require the borrower to maintain at least a certain minimum current ratio.

Acid-Test Ratio (Quick Ratio): Quick Assets Divided by Current Liabilities Quick assets are cash, marketable securities, and net receivables. This ratio is particularly important to short-term creditors since it relates cash and immediate cash inflows to immediate cash outflows. Purchases of inventory on account would make the quick ratio decrease since it does not include inventory. Current liabilities increase, not current assets. Quick assets are current assets minus inventory.

Free Cash Flows Free cash flows are the amount of cash flows available to investors, creditors, and equity owners after the firm has met all operating needs and paid for investments in net fixed assets and net current assets. It is calculated as after-tax operating cash flows minus net fixed asset investment minus net current asset investment. Here the term "free cash flows" does not mean that the cash is "free"; it means that cash is available for other useful purposes.

(B) Asset Management Ratios **Asset management ratios** or **activity ratios** measure the liquidity of certain assets and relate information on how efficiently assets are being utilized.

Inventory Turnover Ratio: Sales Divided by Average Inventory or Cost of Goods Sold Divided by Average Inventory The inventory turnover indicates how quickly inventory is sold. Typically,

a high turnover indicates that an organization is performing well. This ratio can be used in determining whether there is obsolete inventory or if pricing problems exist. The use of different inventory valuation methods (last in, first out [LIFO], first in, first out [FIFO], etc.) can affect the turnover ratio. It is also called inventory utilization ratio. As the obsolete inventory increases, the inventory turnover decreases.

Days Sales Outstanding Ratio: Receivables Divided by Average Sales per Day The days sales outstanding (DSO) ratio indicates the average length of time that a firm must wait to receive cash after making a sale. It measures the number of days sales are tied up in receivables. If the calculated ratio for a company is 45 days, and its sales terms are 30 days, and the industry average ratio is 35 days, it indicates that customers, on the average, are not paying their bills on time. In the absence of a change in the credit policy about sales terms, the higher the company's actual ratio, the greater its need to speed up collection efforts. A decrease in the DSO ratio is an indication of effective collection efforts.

Another related ratio is A/R turnover ratio, which is net credit sales divided by average net trade receivables outstanding. The average receivables outstanding can be calculated by using the beginning and ending balance of the trade receivables. This ratio provides information on the quality of an organization's receivables and how successful it is in collecting outstanding receivables. A fast turnover lends credibility to the current ratio and acid-test ratio.

Fixed Asset Turnover Ratio: Net Sales Divided by Net Fixed Assets Fixed asset turnover ratio shows how effectively the firm uses its fixed assets, such as plant, equipment, machinery, and buildings. Note: Inflation erodes the historical cost base of old assets, thus reporting a higher turnover. This inflation problem makes it hard to compare fixed asset turnover between old and new fixed assets. Assets reported on current value basis would eliminate the inflation problem. Fixed asset turnover is also called fixed assets utilization ratio and is similar to the inventory utilization ratio. A high fixed asset turnover ratio may mean either a firm was efficient in using its fixed assets or that the firm is undercapitalized and could not afford to buy enough fixed assets.

Total Assets Turnover Ratio: Net Sales Divided by Average Total Assets The total assets turnover indicates how efficiently an organization utilizes its capital invested in assets. A high turnover ratio indicates that an organization is effectively using its assets to generate sales. This ratio relates the volume of a business (i.e., sales, revenue) to the size of its total asset investment. In order to improve this ratio, management needs to increase sales, dispose of some assets, or a combination of both.

(C) Debt Management Ratios Debt management ratios or coverage ratios are used in predicting the long-run solvency of organizations. Bondholders are interested in these ratios because they provide some indication of the measure of protection available to bondholders. For those interested in investing in an organization's common stock, these ratios indicate some of the risk, since the addition of debt increases the uncertainty of the return on common stock.

Debt Ratio: Total Debt Divided by Total Assets Debt ratio impacts an organization's ability to obtain additional financing. It is important to creditors because it indicates an organization's ability to withstand losses without impairing the creditor's interest. A creditor prefers a low ratio since it means there is more cushion available to it if the organization becomes insolvent. However, owners prefer a high debt ratio to magnify earnings due to leverage or to minimize loss of control if new stock is issued instead of taking on more debt. Total debt includes both current liabilities and long-term debt.

The capitalization of a lease by a lessee will result in an increase in the debt-to-equity ratio. If a firm purchases a new machine by borrowing the required funds from a bank as a short-term loan, the direct impact of this transaction will be to decrease the current ratio and increase the debt ratio.

Times-Interest-Earned Ratio: Earnings Before Interest and Taxes Divided by Interest Charges The times-interest-earned ratio provides an indication of whether an organization can meet its required interest payments when they become due and not go bankrupt. This ratio also provides a rough measure of cash flow from operations and cash outflow as interest on debt. This information is important to creditors, since a low or negative ratio suggests that an organization could default on required interest payments. This ratio measures the extent to which operating income can decline before the firm is unable to meet its annual interest costs. The ability to pay current interest is not affected by taxes since the interest expense is tax deductible. In other words, the interest expense is paid out of income before taxes are calculated.

Fixed Charge Coverage Ratio: Earnings Before Interest and Taxes Plus Lease Payments Divided by Interest Charges Plus Lease Payments The fixed charge coverage ratio is similar to times-interest-earned ratio except that the former ratio includes long-term lease obligations. When a company's ratio is less than the industry average, the company may have difficulty in increasing its debt.

Cash Flow Coverage Ratio: Earnings Before Interest and Taxes plus Lease Payments plus Depreciation Divided by Interest Charges plus Lease Payments plus Preferred Stock Dividends (Before Tax) plus Debt Repayment (Before Tax) The cash flow coverage ratio shows the margin by which the firm's operating cash flows cover its financial obligations. This ratio considers principal repayment of debt, dividends on preferred stock, lease payments, and interest charges. The reason for putting the dividends on preferred stock and debt repayment amounts on before the tax basis is due to the fact that they are not tax deductible, meaning that they are paid out of the income before taxes are paid.

(D) Profitability Ratios **Profitability ratios** are the ultimate test of management's effectiveness. They indicate how well an organization operated during a year. They are a culmination of many policies and decisions made by management during the current year as well as previous years. Typically these ratios are calculated using sales or total assets. Profitability ratios show the combined effect of liquidity, asset management, and debt management performance on operating results.

Profit Margin on Sales Ratio: Net Income Available to Common Stockholders Divided by Sales The profit margin on sales ratio indicates the proportion of the sales dollar that remains after deducting expenses. Here the net income after taxes is divided by sales to give the profit per dollar of sales.

Basic Earning Power Ratio: Earnings Before Interest and Taxes Divided by Total Assets The basic earning power ratio shows the raw earning power of the firm's assets, before the influence of taxes and impact of the financial leverage. It indicates the ability of the firm's assets to generate operating income. A low "total asset turnover" and low "profit margin on sales" gives a low "basic earning power ratio." Return on investment (ROI) may be calculated by multiplying total asset turnover by profit margin.

Return on Total Assets Ratio: Net Income Available to Common Stockholders Divided by Total Assets The return on total assets (ROA) ratio measures the return on total assets after interest and taxes are paid. The net income used in the equation is the net income after taxes. A low ratio indicates a low basic earning power ratio and a high use of debt.

Another way of looking at the ROA ratio is by breaking it down into subcomponents: net income divided by net sales (i.e., profit margin on sales) as one component and net sales divided by total average assets (i.e., total asset turnover) as another component. This breakdown helps in pinpointing problems and opportunities for improvement.

Return on Common Equity Ratio: Net Income Available to Common Stockholders Divided by Common Equity The return on common equity (ROE) measures the rate of return on common stockholders' investments. The net income used in the equation is the net income after taxes, and common equity is the average stockholders' equity. A low ratio compared to the industry indicates high use of debt. This ratio reflects the return earned by an organization on each dollar of owners' equity invested.

Earnings per Share Ratio: Net Income Minus Current-Year Preferred Dividends Divided by Weighted-Average Number of Shares Outstanding The earnings per share (EPS) ratio is probably the most widely used ratio for evaluating an organization's operating ability. The complexity of the calculation of EPS is determined by a corporation's capital structure.

An organization with no outstanding convertible securities, warrants, or options has a simple capital structure. An organization has a complex structure if it has such items outstanding. Investors should be careful not to concentrate on this number to the exclusion of the organization as a whole. One danger in concentrating on this number is that EPS can easily be increased by purchasing treasury stock that reduces the outstanding shares.

Payout Ratio: Cash Dividends Divided by Net Income or Dividends per Share Divided by Earnings per Share The payout ratio indicates the ability to meet dividend obligations from net income earned. There is a relationship between the payout ratio and the need for obtaining external capital. The higher the payout ratio, the smaller the addition to retained earnings and, hence, the greater the requirements for external capital. This says that dividend policy affects external capital requirements. If d is the dividend payout ratio, $(1 - d)$ is called the earnings retention rate.

Depending on their tax status, certain investors are attracted to the stock of organizations that pay out a large percentage of their earnings. Others are attracted to organizations that retain and reinvest a large percentage of their earnings. Growth organizations typically reinvest a large percentage of their earnings; therefore, they have low payout ratios.

(E) Market Value Ratios Market value ratios relate the firm's stock price to its earnings and book value per share. They show the combined effects of liquidity ratios, profitability ratios, asset management ratios, and debt management ratios. The viewpoint is from outside in (i.e., from an investors' view about the company's financial performance—past and future).

Price/Earnings Ratio: Price per Share Divided by Earnings per Share The price/earnings (P/E) ratio shows how much investors are willing to pay per dollar of reported profits. Financial analysts, stock market analysts, and investors in general use this value to determine whether a stock is overpriced or underpriced. Different analysts have differing views as to the proper P/E ratio for a certain stock or the

future earnings prospects of the firm. Several factors, such as relative risk, trends in earnings, stability of earnings, and the market's perception of the growth potential of the stock, affect the P/E ratio.

P/E RATIOS VERSUS GROWTH VERSUS RISK

- P/E ratios are higher for firms with high growth prospects and low risk.
- P/E ratios are lower for firms with low growth prospects and high risk.

Book Value per Share: Common Equity Divided by Shares Outstanding The book value per share ratio is used as an intermediate step in calculating the market/book ratio. The book value per share ratio is used in evaluating an organization's net worth and any changes in it from year to year. If an organization were liquidated based on the amounts reported on the balance sheet, the book value per share indicates the amount that each share of stock would receive. If the asset amounts on the balance sheet do not approximate fair market value, then the ratio loses much of its relevance.

Market/Book Ratio: Market Price per Share Divided by Book Value per Share Market/book ratio reveals how investors think about the company. Market/book ratio is related to ROE ratio in that high ratio of ROE gives high market/book ratio and vice versa. In other words, companies with higher ROEs sell their stock at higher multiples of book value. Similarly, companies with high rates of return on their assets can have market values in excess of their book values. A low rate of return on assets gives low market/book value ratio.

Examples: Calculation of Financial Ratios

Examples 1 through 3 are based on the following selected data that pertain to a company at December 31, 20X1:

Quick assets	$208,000
Acid-test ratio	2.6 to 1
Current ratio	3.5 to 1
Net sales for 20X4	$1,800,000
Cost of sales for 20X1	$990,000
Average total assets for 20x1	$1,200,000

Example 1

Based on the data, the company's current liabilities at December 31, 20X1, amount to:

a. $ 59,429
b. $ 80,000
c. $342,857
d. $187,200

Choice (**b**) is the correct answer. Computations follow.

$$\frac{\text{Quick assets}}{\text{Current liabilities}} = \text{Acid-test ratio}$$

$$\frac{\$208{,}000}{\text{Current liabilities}} = 2.6$$

$$\text{Current liabilities} = \frac{\$208{,}000}{2.6} = \underline{\underline{\$80{,}000}}$$

Choice (a) is incorrect. This answer incorrectly reflects the computation quick assets ($208,000) divided by the current ratio (3.5). Choice (c) is incorrect. This answer reflects the incorrect computation of average total assets ($1,200,000) divided by the current ratio (3.5). Choice (d) is incorrect. This answer reflects the incorrect computation of quick assets ($208,000) multiplied by the excess of the current ratio (3.5) over the acid-test ratio (2.6).

Example 2

Based on the data listed, the company's inventory balance at December 31, 20X1, is:

a. $ 72,000
b. $187,200
c. $231,111
d. $282,857

Choice **(a)** is the correct answer. Computations follow.

$$\frac{\$208{,}000}{\text{Current liabilities}} = 2.6$$

$$\frac{\$208{,}000}{2.6} = \$80{,}000 = \text{Current liabilities}$$

$$\frac{\text{Current assets}}{\text{Current liabilities}} = \text{Current ratio}$$

$$\frac{\text{Current assets}}{\$80{,}000} = 3.5$$

$$\text{Current Assets} = 3.5 \times \$80{,}000 = \$280{,}000$$

$$\text{Current assets} - \text{Quick assets} = \text{Inventory}$$

$$\$280{,}000 \qquad \$208{,}000 \qquad \$72{,}000$$

Choice (b) is incorrect. This answer reflects the incorrect computation of the current ratio (3.5) minus the acid-test ratio (2.6) multiplied by quick assets ($208,000). Choice (c) is incorrect. This answer reflects the incorrect computation of quick assets ($208,000) divided by the excess of the current ratio (3.5) over the quick ratio (2.6). Choice (d) is incorrect. This answer reflects the incorrect computation of cost of sales ($990,000) divided by the current ratio (3.5).

Example 3

Based on the data listed, the company's asset turnover for 20X1 is:

a. 0.675
b. 0.825
c. 1.21
d. 1.50

Choice **(d)** is the correct answer. Computations follow.

$$\frac{\text{Net sales}}{\text{Average total assets}} = \frac{\$1{,}800{,}000}{\$1{,}200{,}000} = 1.5$$

Choice (a) is incorrect. This answer reflects the incorrect computation of gross profit ($1,800,000 – $990,000) divided by average total assets ($1,200,000). Choice (b) is incorrect. This answer reflects the incorrect computation of cost of sales ($990,000) divided by average total assets ($1,200,000). Choice (c) is incorrect. This answer reflects the incorrect computation of average total assets ($1,200,000) divided by cost of sales ($990,000).

(iv) Limitations of Financial Statement Ratios

Because ratios are simple to compute, convenient, and precise, they are attractive, and a high degree of importance is attached to them. Since these ratios are only as good as the data on which they are based, the next limitations exist:

- The use of ratio analysis could be limiting for large, multidivisional firms due to their size and complexity—two conditions that mask the results. However, they might be useful to small firms.
- Typically, financial statements are not adjusted for price-level changes. Inflation or deflation can have a large effect on the financial data.
- Since transactions are accounted for on a cost basis, unrealized gains and losses on different asset balances are not reflected in the financial statements.
- Income ratios tend to lose credibility in cases where a significant number of estimated items exist, such as amortization and depreciation.
- Seasonal factors affect and distort ratio analysis, which can be minimized by using average figures in calculations.
- Be aware of window-dressing and earnings management techniques used by firms to make them look financially better than what they really are. Management manipulates the financial statements to impress credit analysts and stock market investors (i.e., management fraud).
- Certain off–balance sheet items do not show up on the financial statements. For example, leased assets do not appear on the balance sheet, and the lease liability may not be shown as a debt. Therefore, leasing can improve both the asset turnover and the debt ratios.
- Attaining comparability among organizations in a given industry is an extremely difficult problem, since different organizations apply different accounting procedures. For this reason, auditors must identify the basic differences in accounting from organization to organization and adjust balances to achieve comparability.
- Auditors should not take ratios at their face value since a "good" ratio does not mean that the company is a strong one or that a "bad" ratio means that the company is a weak one. Ratios should be evaluated and interpreted with judgment and experience and considering the firm's characteristics and the industry's uniqueness.

(e) Types of Debt and Equity

(i) Types of Debt

Debt is of two types: short-term debt and long-term debt. Debt maturities affect both risk and expected returns. For example, short-term debt:

- Is riskier than long-term debt.
- Is less expensive than long-term debt.
- Can be obtained faster than long-term debt.
- Is more flexible than long-term debt.

(A) Sources of Short-Term Financing By definition, short-term debt (credit) is any liability originally scheduled for payment within one year. The four major sources of short-term credit are: (1) accruals, (2) A/P, (3) bank loans, and (4) commercial paper. The order of short-term credit sources is shown next from both cost and importance viewpoints.

In the order of importance	In the order of cost
A. Trade credit (most important)	A. Trade credit (free, no interest paid)
B. Bank loans	B. Accruals
C. Commercial paper	C. Commercial paper
D. Accruals (least important)	D. Bank loans (not free, interest paid)

Trade Credit Trade credit is granted by suppliers of goods as a sales promotion device. All firms, regardless of their size, depend on A/P or trade credit as a source of short-term financing. Small firms do rely more heavily on trade credit than larger firms due to the former's inability to raise money from other sources. Trade credit, a major part of current liability, is an interfirm debt arising from credit sales and recorded as an A/R by the seller and as an A/P by the buyer. Trade credit is a spontaneous source of financing arising from normal course of business operations.

When payment terms are extended, the amount in A/P is expanded to provide an additional source of financing. Therefore, lengthening the credit period generates additional financing.

Payment terms vary and usually call for "net 30," meaning that it must pay for goods 30 days after the invoice date. Other terms include "1/10, net 30" which means that a 1% discount is given if payment is made within 10 days of the invoice date, but the full invoice amount is due and payable within 30 days if the discount is not taken. The finance manager has a choice of taking or not taking the discount and needs to calculate the cost of not taking discounts on purchases. The equation is

$$\text{Percentage cost of not taking discount} = \frac{\text{Discount percent}}{100\% - \text{Discount \%}} \times \frac{360}{A - B}$$

where A = Days credit is outstanding
B = Discount period

Example: Cost of Not Taking a Discount

The approximate cost of not taking a discount when the payment terms are 1/10, net 30, is calculated as follows:

$$\text{Percentage cost of not taking discount} = \frac{1}{100\% - 1\%} \times \frac{360}{30 - 10} = 0.18 = 18\%$$

By paying late (stretching A/P), the cost of trade credit is reduced. This is shown next. When a 30-day bill is paid in 60 days, the approximate cost drops from 18% to 7.2%. That, is $1/99 \times 360/(60 - 10) = 0.072 = 7.2\%$.

KEY CONCEPTS TO REMEMBER: Cost of Trade Discounts

- The cost of not taking trade discounts can be substantial.
- The cost can be doubled when payment (credit) terms are changed from 1/10, net 30 to 1/10, net 20.
- The cost can be doubled when payment (credit) terms are changed from 1/10, net 30 to 2/10, net 30.
- The cost can be quadrupled when payment (credit) terms are changed from 1/10, net 30 to 2/10, net 20.
- The cost can be reduced by paying late (i.e., from 2/10, net 30 to 2/10, net 60).

A firm's policy with regard to taking or not taking trade discounts can have a significant effect on its financial statements. A dichotomy exists here in terms of taking discounts or not taking discounts. Careful analysis needs to be performed showing relevant costs and its effects on net income.

Decision Conditions

1. If the company does not take discounts (i.e., uses maximum trade credit), its interest expense will be zero (i.e., no borrowing is necessary), but it will have an expense equivalent to lost discounts.
2. If the company does take discounts (i.e., borrows money from bank), it will incur interest expense on the loan, but it will avoid the cost of discounts lost. The company gives up some of the trade credit, and it has to raise money from other sources, such as bank credit, common stock, or long-term bonds.

Decision Rules

1. If the discount amount lost exceeds the interest expense, a take-discounts policy would result in a higher net income and eventually a higher stock price.
2. If the interest expense exceeds the discount amount lost, a does-not-take-discounts policy would result in a higher net income and eventually a higher stock price.

Bank Loans Bank loans appear on firms' balance sheets under the notes payable account category. A promissory note is signed by the borrower (customer) specifying the amount borrowed, the percentage interest rate, the repayment schedule, any collateral, and any other terms and conditions. Banks require a compensating balance in the form of a minimum checking account balance equal to a specified percentage (i.e., 10–20%) of the face amount of the loan. A compensating balance raises the effective interest rate on the loan.

Examples of Bank Loan Features

- Promissory note
- Compensating balance
- Line of credit
- Revolving credit agreement

Banks also give a line of credit to a borrower, which works like a credit card limit. A line of credit can be based on either formal or informal understanding. It includes the maximum amount of credit the bank will extend to the borrower. A revolving credit agreement, which is similar to a line of credit, is a formal line of credit often used by large firms. The bank has a legal obligation to honor a revolving credit agreement; no legal obligation exists under the line of credit.

The cost of a bank loan (i.e., interest rate) varies depending on economic conditions and Federal Reserve (Fed) money supply policy. Generally, interest rates are higher for riskier borrowers and for smaller loans due to fixed costs of servicing the loan. If a firm is financially strong, it can borrow at the prime rate, which traditionally has been the lowest rates bank charge. If a firm is financially weak, the bank will charge higher than prime rate to compensate for the risk involved.

KEY CONCEPTS TO REMEMBER: Loan Demand and Interest Rates

- When the economy is weak (i.e., loan demand is weak), the Fed increases the money supply. Consequently, the interest rates on all types of loans decline.
- When the economy is strong (i.e., loan demand is strong), the Fed decreases the money supply. Consequently, the interest rates on all types of loans increases.

Interest rates on bank loans are quoted in three ways: simple interest, discount interest, and add-on interest. Each method is discussed briefly.

Simple (regular) interest. In a simple interest loan, the borrower receives the face value of the loan and then repays the principal and interest at maturity.

Effective rate = Interest/Amount received

If a loan period is one year or more, the nominal (stated) rate equals the effective rate. If a loan period is less than one year, the effective rate is higher than nominal (stated) rate.

Discount interest. In a discount interest loan, the borrower receives less than the face value of the loan since the bank deducts the interest in advance.

Effective rate = Interest/Amount received

Because of discounting, the effective rate is always higher than a simple interest loan regardless of the loan period. However, the discount interest imposes less of a penalty on a shorter-term than on a longer-term loan because the interest is paid closer to the average date of use of the funds (half the life of the loan).

Add-on interest. Small installment loans employ the add-on interest method. The interest is calculated based on the nominal rate and then added to the amount received to obtain the loan's face value.

Effective rate = Interest/0.5 (Amount received)

The effective rate can be almost double the stated rate since the average amount actually outstanding is less than the original amount of the loan.

The situation is different when compensating balances are introduced to the simple interest method and discount interest method. In general, compensating balances tend to raise the effective

interest rate on a loan because some money is tied up in a checking account (i.e., cannot be used). There are two exceptions: (1) If the firm can use transaction balances as compensating balances, the effective interest rate will be less than otherwise; and (2) if the firm can earn interest on its bank deposits, including the compensating balance, the effective interest rate will be decreased.

Commercial Paper Commercial paper represents short-term, unsecured promissory notes of large, strong firms and is highly liquid in nature. The interest rate charged on commercial paper is somewhat below the prime rate, and its maturity ranges from two to six months. Even though compensating balances are not required for commercial paper, its effective interest rate is higher due to the loan commitment fees involved.

Firms issuing commercial paper are required by commercial paper dealers to have unused revolving credit agreements to back up their outstanding commercial paper. A commitment fee is charged on the unused credit line.

Unlike bank loans, the commercial paper market is impersonal. However, the commercial paper market is flexible and provides a wide range of credit sources generally available to financially strong firms with low credit risks.

Accruals Accruals are short-term liabilities arising from wages owed to employees and taxes owed to government. These accruals increase automatically as a firm's operations expand; hence little control exists over their levels. No explicit interest is paid on funds raised through accruals.

(B) Use of Security in Short-Term Financing The security agreement of the Uniform Commercial Code (UCC) provides guidelines for establishing loan security. Secured loans are expensive due to record-keeping costs. Financially weak companies are required to put up some type of collateral to protect the lender, while financially strong companies generally are not so required, even though they are encouraged to do so. Most commonly used collateral for short-term credit is A/R and inventories, which are described in Exhibit 7.11.

Collateral for short-term loans	Collateral for long-term loans
Accounts receivable	Land
Inventories	Building
Stocks	Equipment
Bonds	Stocks
	Bonds

EXHIBIT 7.11 Collateral for Short-Term and Long-Term Loans

Accounts Receivable Financing A/R financing involves either the pledging of receivables or the selling of receivables (i.e., factoring) to obtain a short-term loan. Either commercial banks or industrial finance companies usually are involved in pledging and factoring, and a legally binding agent is established between the borrower and the lender (see Exhibit 7.12).

The expensive operation of pledging and factoring functions today will become less expensive tomorrow due to automation and use of debit cards and credit cards. This makes it affordable for small companies to finance their receivables. When a credit card is used to purchase an item, the seller is in effect factoring receivables.

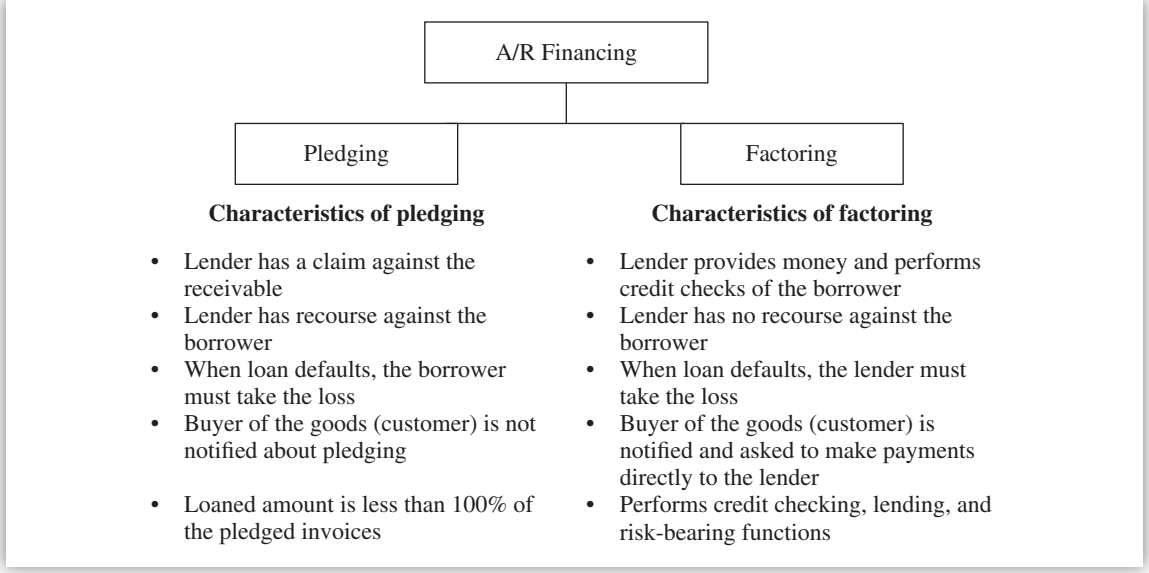


EXHIBIT 7.12 Accounts Receivable Financing Methods

Advantages and Disadvantages of A/R Financing Advantages and disadvantages of A/R financing are listed next.

Advantages

Flexibility because the financing is tied to the growth of receivables. As sales increase, financing increases. Receivables are put to better use than would be the case otherwise. Benefit of an in-house credit department without having one.

Disadvantages

Administrative costs could be higher to handle a large volume of invoices with small dollar amounts. Trade creditors may object to selling their goods on credit because receivables (noncash assets) are being pledged or factored. They may have an uneasy feeling about this type of financing arrangement.

Inventory Financing Inventory financing involves the use of inventory as a security to obtain a short-term loan. Three methods exist: inventory blanket liens, trust receipts, and warehouse receipts (see Exhibit 7.13).

Advantages and Disadvantages of Field Warehouse Financing Advantages and disadvantages of field warehouse financing are listed next.

Advantages

Flexibility because the financing is tied to the growth of inventories. More sales means more inventory buildup is required and more financing is needed. A convenient method is loan collateral. Better inventory control and warehousing practices, which in turn save handling costs, insurance charges, and theft losses.

Disadvantages

Extensive amount of paperwork is required. Goods are physically separated using fences and signs. The cost of supervision by a custodian of the field warehousing company is high, especially for small firms obtaining the loan.

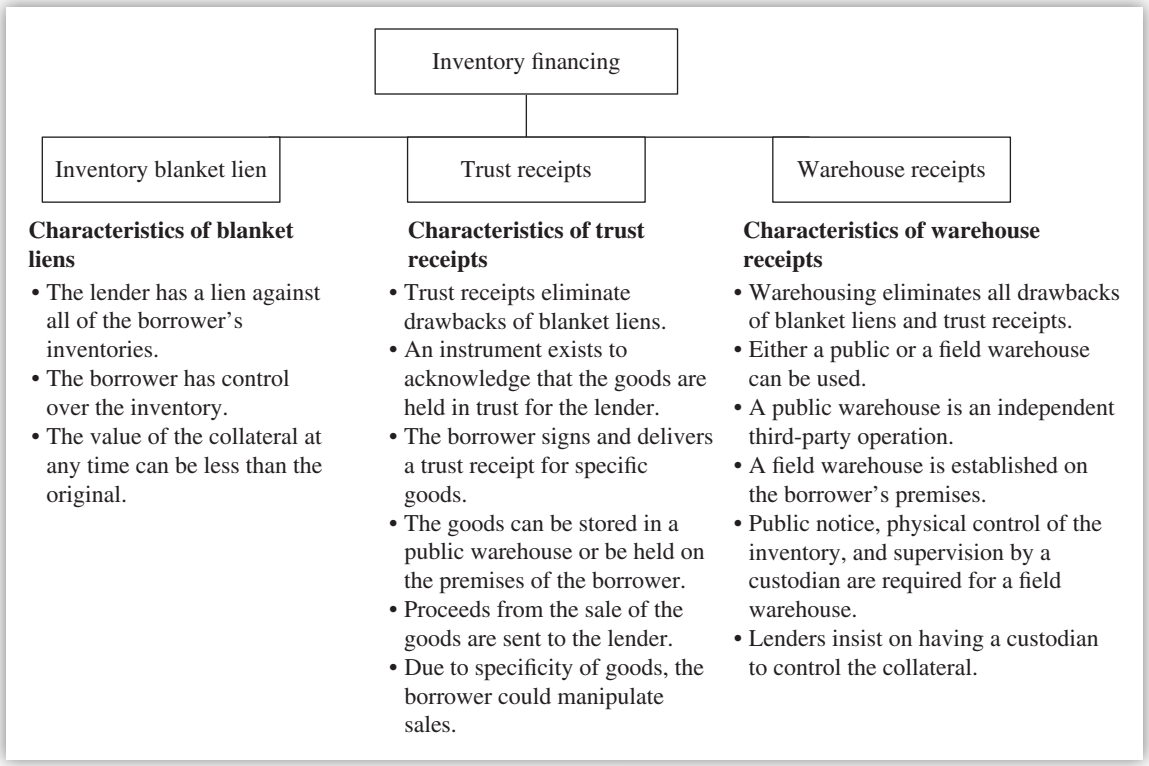


EXHIBIT 7.13 Inventory Financing Methods

(C) Long-Term Debt Long-term debt is often called funded debt, a term used to define the replacement of short-term debt with securities of longer maturity (e.g., stocks, bonds). Many types of long-term debt instruments are available, including term loans, bonds, secured notes, unsecured notes, marketable debt, and nonmarketable debt. Term loans and bonds are discussed next.

Term Loans A term "loan" is a contract under which a borrower agrees to make a series of payments (interest and principal) at specific times to the lender. Most term loans are amortized, which means they are paid off in equal installments over the life of the loan, ranging from 3 to 15 years. Amortization protects the lender against inadequate loan provisions made by the borrower.

Since the agreement is between the lender and the borrower, documentation requirements are lower, the speed and future flexibility are greater, and the cost is lower compared to a public offering involved in a stock or bond issue. The interest rate on a term loan can be either fixed or variable, and lenders are reluctant to make long-term, fixed rate loans.

KEY CONCEPTS TO REMEMBER: Term Loans

- If a fixed rate is used, it is set close to the rate on bonds of equivalent maturity and risk.
- If a variable rate is used, it is set at a certain number of percentage points over the prime rate, commercial paper rate, Treasury bill rate, Treasury bond rate, or London Interbank Offered Rate (LIBOR). When the index rate goes up or down, the rate charged on the outstanding balance will vary accordingly.

Bonds A bond is a long-term contract (7 to 10 years or more) under which a borrower agrees to make payments (interest and principal) on specific dates to the holder of the bond. The interest rates paid on bonds can be fixed or variable (floating rate bonds); generally they are fixed.

Some debts have specific contractual requirements to meet. The effective cost of the debt, is high and many restrictions are placed in the debt contracts, which limits a firm's future flexibility. In order to protect the rights of the bondholders and the issuing firm, a legal document called "indenture" is created, which includes restrictive covenants. A trustee, usually a bank, is assigned to represent the bondholders. The role of the trustee is to enforce the terms of the indenture and to ensure compliance with restrictive covenants.

WHAT IS INCLUDED IN RESTRICTIVE COVENANTS?

- Conditions under which the issuer can pay off the bonds prior to maturity
- The level at which the issuer's times-interest-earned ratio must be maintained if the firm is to sell additional bonds
- Restrictions against the payment of dividends when earnings fall below a certain level

Most bonds contain a **call provision** that gives the issuing firm the right to call the bonds before maturity for redemption. The bondholder is paid an amount greater than par value (call premium) for the bond when it is called. The call premium is set equal to one year's interest if the bond is called during the first year, and the premium declines at a constant rate of I/N each year thereafter, where I equals annual interest and N equals original maturity in years.

TERM LOANS VERSUS BONDS

- Bonds and term loans are similar in that both require payments of interest and principal amounts on specific dates.
- Only one lender is involved in a term loan. Thousands of investors are involved in a bond issue.
- A bond issue is advertised and sold to many investors. A term loan is not advertised and only one borrower is involved.
- Syndicates of many financial institutions can grant very large term loans.
- A bond issue can be sold to one or a few lenders (privately placed) for speed, flexibility, and low issuance costs.

Another example of specific debt contract features is **sinking fund** requirements. A sinking fund is a provision that requires an annual payment designed to amortize a bond or preferred stock issue. It retires a portion of the bond issue each year. It can also be viewed as buying back a certain percentage of the issue each year. Annual payments are a cash drain on the firm, and nonpayment could cause default or force the company into bankruptcy. The firm may deposit money with a trustee who will retire the bonds when they mature.

KEY CONCEPTS TO REMEMBER: Call Provision and Sinking Fund

- A bond without a call provision will protect the bondholder. The investor is not subject to interest rate fluctuations.
- A bond with a sinking fund call provision will not protect the bondholder when interest rate falls. The investor loses money on interest.
- Bonds with a sinking fund provision are safer than bonds without such a provision. This results in lower coupon rates.

The sinking fund retirement is handled either by calling in for redemption (at par) a certain percentage of the bonds each year or by buying the required amount of bonds on the open market. A sinking fund call requires no call premium; a refunding operation does require such a premium. A sinking fund requires that a small percentage of the issue is callable in any one year.

The refunding operation works as follows: When a firm sold bonds or preferred stock at high interest rates, and if the issue is callable, the firm could sell a new issue at low interest rates.Then the firm could retire the expensive old issue. This refunding operation reduces interest costs and preferred dividend expenses.

INTEREST RATES VERSUS BOND PRICES

- There is an inverse relationship between bond prices and interest rates.
- If interest rates are increased, the firm will buy bonds in the open market at a discount.
- If interest rates are decreased, the firm will call the bonds.

Types of Long-Term Bonds

Mortgage bonds. Under a mortgage bond, the corporation pledges certain fixed assets as security for the bond. Mortgage bonds can be of two types: senior (first) mortgage bonds and junior (second) mortgage bonds. Second mortgage bondholders are paid only after the first mortgage bondholders have been paid off in full. All mortgage bonds are written subject to an indenture. Details regarding the nature of secured assets are contained in the mortgage instrument. From the viewpoint of the investor, mortgage bonds provide lower risk and junk bonds provide greater risk.

BOND RATING CRITERIA

- Debt ratio
- Times-interest-earned ratio
- Current ratio
- Fixed charge coverage ratio
- Mortgage or other provisions
- Sinking fund requirements

Debentures. A debenture is an unsecured bond. Consequently, it provides no lien against specific property as security for the obligation. Debenture holders are general creditors. Financially strong companies do not need to put up property as security when they issue debentures. Debentures can be subordinate or not. In the event of liquidation, reorganization, or bankruptcy, subordinate debt has claims on assets only after senior debt has been paid off. Subordinate debentures may be subordinated either to designated notes payable or to all other debt.

Convertible bonds. Convertible bonds are securities that are convertible into shares of common stock, at a fixed price, at the option of the bondholder. Convertible bonds have a lower coupon rate than nonconvertible debt and have a chance for capital gains.

Warrants. Warrants are options that permit the holder to buy stock for a stated price, thereby providing a capital gain if the price of the stock rises. Bonds that are issued with warrants, such as convertible bonds, carry lower coupon rates than straight bonds.

Income bonds. As the name implies, income bonds pay interest only when the interest is earned. These bonds are safer to a company but riskier to an investor than "regular" bonds.

Putable bonds. Putable bonds may be turned in and exchanged for cash at the holder's option. The put option can be exercised only if the issuer is being acquired or is increasing its outstanding debt or other specified action.

Treasury bonds. A treasury bond will have the lowest risk and low opportunity for return to an investor. It has the highest interest rate risk at the date of issue to an issuer (see Exhibit 7.14).

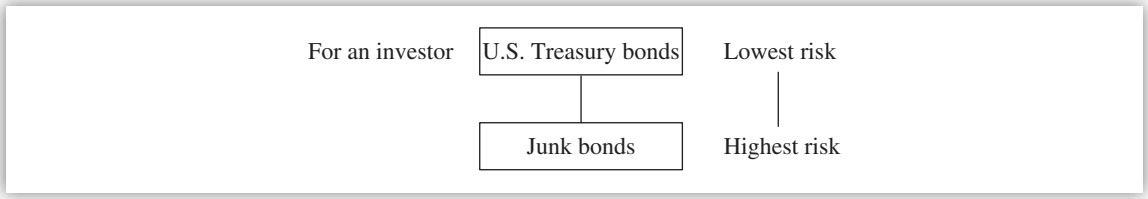


EXHIBIT 7.14 Bonds and Risks

Indexed bonds. Countries faced with high inflation rates issue indexed bonds, also known as purchasing power bonds. The interest paid is based on an inflation index (e.g., Consumer Price Index) so that the interest paid rises automatically when the inflation rate rises. This bond protects the bondholder against inflation.

Floating rate bonds. The interest rate on floating rate bonds fluctuates with shifts in the general level of interest rates. The interest rate on these bonds is adjusted periodically, and it benefits the investor and the lender. Corporations also benefit from not having to commit themselves to paying a high rate of interest for the entire life of the loan.

Zero-coupon bonds. The major attraction in zero-coupon bonds is capital appreciation rather than interest income. Therefore, zero-coupon bonds pay no interest and are offered at a discount below their par values. Both private and public organizations are offering zero-coupon bonds to raise money. Zero-coupon bonds are also called original issue discount bonds.

Junk bonds. Junk bonds are high-risk, high-yield bonds issued to finance a leveraged buyout, a merger, or a troubled company. In junk bond deals, the debt ratio is high, so bondholders share as much risk as stockholders would. Since the interest expense on bonds is tax deductible, it increases after-tax cash flows of the bond issuer.

So many different types of long-term securities are available because different investors have different risk/return trade-off preferences. Different securities are issued to accommodate different tastes of investors and at different points in time. Short-term U.S. Treasury bills are risk-free and low-return securities (they act as a reference point); warrants are high-risk and high-return securities.

(D) Factors Influencing Long-Term Financing Decisions Long-term financing decisions require a great deal of planning since a firm commits itself for many years to come. The long-term nature combined with uncertainty makes long-term financing risky, requiring careful consideration of all factors involved. Examples of important factors are listed next.

- **Target capital structure.** A firm should compare its actual capital structure to its target structure and keep them in balance over a longer period of time. Exact matching of capital structure is not economically feasible on a yearly financing basis due to increased flotation costs involved. It has been shown that small fluctuations about the optimal capital structure have little effect either on a firm's cost of debt and equity or on its overall cost of capital.
- **Maturity matching.** The maturity-matching concept proposes matching the maturity of the liabilities (debt) with the maturity of the assets being financed. This factor has a major influence on the type of debt securities used.
- **Interest rate levels.** Consideration of both absolute and relative interest rate levels is crucial in making long-term financing decisions. The issuance of a long-term debt with a call provision is one example where the interest rate fluctuates. The callability of a bond permits the firm to refund the issue, should interest rates drop. Companies base their financing decisions on expectations about future interest rates.
- **The firm's current and forecasted financial conditions.** The firm's financial condition, earnings forecasts, status of R&D programs, and introduction of new products all have a major influence on what type of long-term security is issued. For example, these decision rules apply:
  - If management forecasts higher earnings, the firm could use debt now rather than issuing common stock. After earnings have risen and pushed up the stock price, the firm should issue common stock to restore the capital structure to its target level.
  - If a firm is financially weak but forecasts better earnings, permanent financing should be delayed until conditions have improved.
  - If a firm is financially strong now but forecasts poor earnings, it should use long-term financing now rather than waiting.
- **Restrictions in existing debt contracts and availability of collateral.** Restrictions on the current ratio, debt ratio, times-interest-earned ratio, and fixed charge coverage ratio can also restrict a firm's ability to use different types of financing at a given time. Also, secured long-term debt will be less costly than unsecured debt. Firms with large amounts of fixed assets (with a ready resale value) are likely to use a relatively large amount of debt.

(ii) Types of Equity

When management decides to acquire new assets, it has the option of financing these assets with equity, debt, or a combination. A good financial management policy is presented next.

- Long-term assets should be financed with long-term capital.
- Short-term assets should be financed with short-term capital.

The term "common equity" means the sum of the firm's common stock, additional paid-in capital, preferred stock, and retained earnings. Common equity is the common stockholders' total investment in the firm. The sources of long-term capital are shown in Exhibit 7.15.

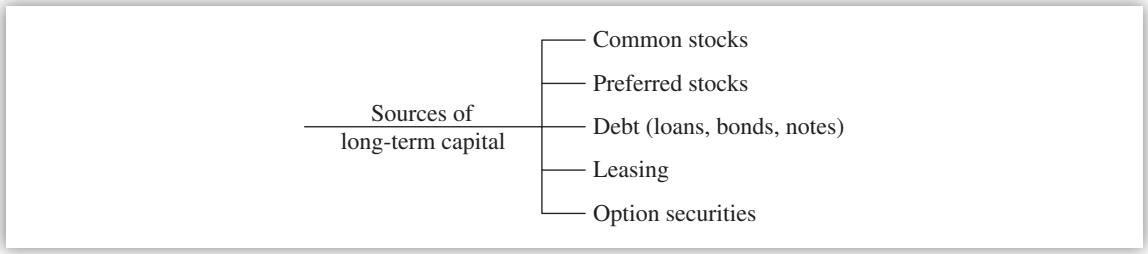


EXHIBIT 7.15 Sources of Long-Term Capital

Common stocks and preferred stocks are discussed in this section. Debt was discussed in the previous section, and leasing was presented earlier in this chapter.

(A) Common Stocks The common stockholders are the owners of a corporation. Common stock is the amount of stock management has actually issued (sold) at par value. Par value is the nominal or face value of a stock and is the minimum amount for which new shares can be issued. The component "additional paid-in capital" represents the difference between the stock's par value and what new stockholders paid when they bought newly issued shares. Retained earnings are the money that belongs to the stockholders and that they could have received in the form of dividends. Retained earnings are also the money that was plowed back into the firm for reinvestment.

Book value of the firm = Common stock + Paid-in capital + Retained earnings = Common equity

Book value per share = Book value of the firm divided by common shares outstanding

It is interesting to note that par value, book value, and market value will never be equal due to conflicting relationships.

KEY CONCEPTS TO REMEMBER: Relationships among Book Value, Par Value, and Market Value

- If a company had lost money since its inception, it would have had negative retained earnings, the book value would have been below par value, and the market price could have been below the book value.
- When a stock is sold at a price above book value per share, the book value increases.
- When a stock is sold at a price below book value per share, the book value decreases.

Most firms have one type of common stock while others may have multiple types of stock called classified stock. Usually newer firms issue classified stock to raise funds from outside sources. For example, Class A stock may be sold to the public with a dividend payment but no voting rights. Class B stock may be kept by the founder of the firm to gain control with full voting rights. A restriction might be placed on Class B stock not to pay dividends until the firm reaches a predesignated retained earnings level.

Legal Rights of Common Stockholders Since the common stockholders are the owners of a firm, they have these rights: the right to elect the firm's directors and the right to remove the

management of the firm if they decide a management team is not effective. Stockholders can transfer their right to vote to a second party by means of an instrument known as a proxy. A proxy fight is a situation where outsiders plan to take control of the business by requesting that stockholders transfer their rights to outsiders in order to remove the current management and to bring in a new management team.

Common stock holders have preemptive rights to purchase any additional shares sold by the firm. Preemptive rights protect the power of control of current stockholders and protect stockholders against a dilution of stock value. Selling common stock at a price below the market value would dilute its price. This would transfer wealth from present stockholders to new stockholders. Preemptive rights prevent such transfer.

Put and Call Options A put option is the right to sell stock at a given price within a certain period. A call option is the right to purchase stock at a given price within a certain period. Selling a put option could force the company to purchase additional stock if the option is exercised. The holder of a put option for a particular common stock would make a profit if the option is exercised during the option term after the stock price has declined below the put price. A warrant option gives the holder a right to purchase stock from the issuer at a given price.

Exhibit 7.16 presents the advantages and disadvantages associated with common stock financing.

Advantages of common stock financing	Disadvantages of common stock financing
It gives the benefits of ownership and expected returns in terms of dividends and capital gains.	It gives voting rights and control to new stockholders when a stock is sold.
It does not obligate the firm to make dividend payments to stockholders; dividends are optional and dependent on earnings, investment plans, and management practices. This gives flexibility to management.	It gives new stockholders the right to share in the income of the firm.
It has no fixed maturity date.	It increases the cost of underwriting and distributing common stock. Flotation costs are higher than incurred for debt.
It provides a cushion against losses from the creditors' viewpoint since it increases the creditworthiness of the firm. It lowers the firm's cost of debt due to a good bond rating.	Its average cost of capital will be higher when a firm has more equity than is called for in its optimal capital structure.
It provides the investor with a better hedge against unanticipated inflation.	Its dividend payments are not tax deductible for corporations.
It provides financing flexibility in that it permits companies to finance with common stock during good times and to finance with debt during bad times. This practice is called "reserve borrowing capacity."	

EXHIBIT 7.16 Advantages and Disadvantages of Common Stock Financing

(B) Preferred Stock Preferred stock is issued to raise long-term capital for many reasons: When neither common stock nor long-term debt can be issued on reasonable terms; during adverse

business conditions, a firm can issue preferred stock with warrants when the common stock is depressed in order to bolster the equity component of a firm's capital structure; a firm can issue convertible preferred stock in connection with mergers and acquisitions (M&A); and a firm can issue a floating-rate preferred stock to stabilize the market price.

Preferred stock is the stock whose dividend rate fluctuates with changes in the general level of interest rates. Thus, this stock is good for liquidity portfolios (e.g., marketable securities). It is a neat way to obtain new capital at a low cost due to its floating dividend rates, stable market price, and tax exemption for dividends received.

Under U.S. tax laws, if preferred stock with conversion privilege is exchanged for the acquired company's common stock, this constitutes a tax-free exchange of securities (i.e., no gain or loss is recognized for tax purposes). Also, if the buyout was for cash, the acquired stockholders would have to pay capital gain taxes.

Preferred stock is a hybrid stock, meaning that it is similar to bonds in some respects and similar to common stock in others. Therefore, preferred stock can be classified either as bonds or common stock (see Exhibit 7.17).

Preferred stocks as bonds (debt)	Preferred stocks as common stocks (equity)
Like bonds, preferred stock has a par value and a call provision.	Like most common stock, preferred stock has a par value.
Preferred dividends are fixed similar to interest payments on bonds and must be paid before common stock dividends can be paid.	Like common stock, preferred stocks have no maturity date and are not callable. Hence they are perpetuity stocks.
During financial difficulty, preferred dividends can be omitted without leading the firm to bankruptcy.	Unlike common stock, most preferred stock requires dividend payments. This reduces earnings available for common stock shareholders. Preferred stock dividends must be paid before common stock dividends can be paid.
Financial analysts sometimes treat preferred stock as debt.	Like common stock, preferred stock carries a voting right to vote for director.
Like debt, preferred stocks have coverage requirements for the amount of preferred stock and the level of retained earnings.	Unlike common stock, there is no share in control of the firm.
Preferred stock may be redeemed at a given time, at the option of the holder, or at a time not controlled by the issuer—called transient preferreds.	Like common stock dividends, preferred dividends can be omitted without bankrupting the firm.
	Financial analysts sometimes treat preferred stock as common stock.

EXHIBIT 7.17 Characteristics of Preferred Stock

Preferred stock is usually reported in the equity section of the balance sheet under "preferred stock" or "preferred equity." Accountants and financial analysts treat the preferred stock differently. Accountants treat preferred stock as equity, and financial analysts treat it as equity or debt, depending on who benefits from the analysis being made. Preferred stock has an advantage in that it has a higher priority claim than common stock (see Exhibit 7.18).

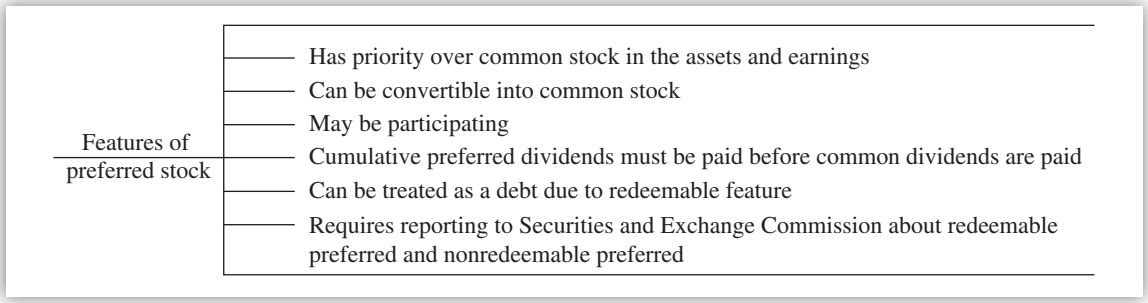


EXHIBIT 7.18 Features of Preferred Stock

KEY CONCEPTS TO REMEMBER: Preferred Stock From Whose Viewpoint?

- From the common stockholders' point of view, preferred stock is similar to debt due to the fixed dividend payment and reduced earnings for common stock.
- From the debt holder's point of view, preferred stock is similar to common equity due to the high priority of the debt holder's claim on assets when the firm is liquidated.
- From management's point of view, preferred stock is safer to use than debt since it will not force the company to bankruptcy for lack of dividend payment. Loan defaults would force the company to bankruptcy.

Exhibit 7.19 shows the relative priorities over assets when the firm is in the liquidation stage.

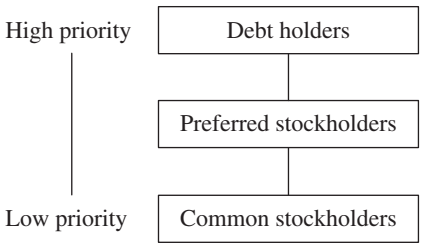


EXHIBIT 7.19 Relative Priorities over Assets

Major Provisions of Preferred Stocks Major provisions of preferred stocks are listed next.

- Priority to assets and earnings
- Par value
- Cumulative dividends
- Convertibility into common stock
- Voting rights
- Participation in sharing the firm's earnings
- Sinking fund requirements
- Maturity date
- Call provisions

Some of these provisions are explained next:

- **Cumulative dividends.** All preferred dividends in arrears must be paid before common dividends can be paid. This is a protection feature for preferred stock to receive a preferred position and to avoid paying huge common stock dividends at the expense of paying stipulated annual dividend to the preferred stockholders.
- **Sinking fund requirements.** Most newly issued preferred stocks have sinking fund requirements that call for the purchase and retirement of a given percentage (e.g., 2–3%) of the preferred stock each year.
- **Call provisions.** A call provision gives the issuing corporation the right to call in the preferred stock for redemption. A call premium may be attached where a company has to pay more than par value when it calls the preferred stock.

Pros and Cons of Preferred Stock from Issuer and Investor Viewpoints From an issuer's viewpoint, the **advantages** of financing with preferred stock are: fixed financial cost, no danger of bankruptcy if earnings are too low to meet fixed charges, and avoidance of sharing control of the firm with new investors.

From an issuer's viewpoint, the **disadvantage** of financing with preferred stock is a higher after-tax cost of capital than debt due to nondeductibility of preferred dividends. The lower a company's tax bracket, the more likely it is to issue preferred stock.

From an investor's viewpoint, the **advantages** of financing with preferred stock are: steadier and more assured income than common stock, preference over common stock in the case of liquidation, and tax exemption for preferred dividends received.

From an investor's viewpoint, the **disadvantages** of financing with preferred stock are: no legally enforceable right to dividends, even if a company earns a profit; and for individual investors, after-tax bond yields could be higher than those on preferred stock, even though the preferred stock is riskier.

(f) Financial Instruments

Financial instruments (currency and credit derivatives) are used by large and small businesses in every industry to hedge against financial risk. One means to hedge currency exposure and risk is through the currency market, which includes forward contracts, futures contracts, currency options, currency swaps, and credit derivatives. In addition, hidden financial reporting risks and financial engineering topics are discussed.

(i) Forward Contracts

In the forward exchange market, one buys a forward contract for the exchange of one currency for another at a specific future date and at a specific exchange ratio. This differs from the spot market, where currencies are traded for immediate delivery. A forward contract provides assurance of being able to convert into a desired currency at a price set in advance. A foreign currency sells at a **forward discount** if its forward price is less than its spot price. If the forward price exceeds the spot price, it is said to sell at a **forward premium**. Forward contracts provide a two-sided hedge against currency movements. Forward contracts are settled only at expiration, and they can be issued at any size.

(ii) Futures Contracts

A futures contract is a standardized agreement that calls for delivery of a currency at some specified future date. These contracts are formed with a clearinghouse, not directly between the two parties. Futures contracts provide a two-sided hedge against currency movements.

Each day, the futures contract is marked to market, meaning it is valued at the closing price. Price movements affect buyer and seller in opposite ways. Every day there is a winner and a loser, depending on the direction of price movement. The loser must come up with more margin (a small deposit), while the winner can draw off excess margin. Future contracts come only in multiples of standard-size contracts.

(iii) Currency Options

An **option** is a contract that gives its holder the right to buy or sell an asset at some predetermined price within a specified period of time. Pure options (financial options) are created by outsiders (investment banking firms) rather than by the firm itself; they are bought and sold by investors or speculators. The leverage involved makes it possible for speculators to make more money with just a few dollars. Also, investors with sizable portfolios can sell options against their stocks and earn the value of the options (minus brokerage commissions) even if the stocks' prices remain constant. Option contracts enable the hedging of one-sided risk. Only adverse currency movements are hedged, either with a call option to buy the foreign currency or with a put option to sell it.

Both the value of the underlying stock and the striking price of the option are very important in determining whether an option is in the money or out of the money. If an option is out of the money on its expiration date, it is worthless. Therefore, the stock price and the striking price are important for determining the market value of an option. In fact, options are called derivative securities because their values are dependent on, or derived from, the value of the underlying asset and the striking price. In addition to the stock's market price and the striking price, the value of an option also depends on the option's time to maturity, the level of strike price, the risk-free rate, and the variability of the underlying stock's price. The higher the strike price, the lower the call option price. The higher the stock's market price in relation to the strike price, the higher will be the call option price. The longer the option period, the higher the option price and the larger its premium. The exercise value of an option is the maximum of the current price of the stock minus the strike price. The price of an option is the cost of stock minus the PV of portfolio. The *Black-Scholes model* is used to estimate the value of a call option.

Warrants are options issued by a company that give the holder the right to buy a stated number of shares of the company's stock at a specified price. Warrants are distributed along with debt, and they are used to induce investors (a sweetener) to buy a firm's long-term debt at a lower interest rate than otherwise would be required.

Real options are used for investment in real assets. Their value is determined as follows:

$$\text{Project discounted cash flow value} = (\text{Cash flows})/(1 + \text{Risk-free cash flow})$$

(iv) Currency Swaps

A swap exchanges a floating-rate obligation for a fixed rate one, or vice versa. There are two types of swaps: currency swaps and interest rate swaps. With the currency swaps, two parties exchange interest obligations on debt denominated in different currencies. At maturity, the principal amounts are exchanged, usually at a rate of exchange agreed on in advance. With an interest rate swap, interest-payment obligations are exchanged between two parties, but they are denominated in the same currency. There is not an actual exchange of principal. If one party defaults, there is no loss of principal per se. However, there is the opportunity cost associated with currency movements after the swap's initiation. These movements affect both interest and principal payments. In this respect, currency swaps are more risky than interest rate swaps,

where the exposure is only to interest. Currency swaps are combined with interest rate swaps; there is an exchange of fixed rate for floating rate payments where the two payments are in different currencies. Financing hedges provide a means to hedge on a longer-term basis, as do currency swaps.

The swap can be longer term in nature (15 years or more) than either forward or futures contracts (5 years). Swaps are like a series of forward contracts corresponding to the future settlement dates at which difference checks are paid. However, a comparable forward market does not exist, nor do lengthy futures or options contracts.

The most common swap is the floating/fixed rate exchange. The exchange itself is on a net settlement basis. That is, the party that owes more interest than it receives in the swap pays the difference. A basis swap is another popular swap where two floating rate obligations are exchanged.

Various options exist for swap transactions, which are known as swaptions. One is to enter a swap at a future date. The terms of the swap are set at the time of the option, and they give the holder the right, but not the obligation, to take a swap position.

(v) Credit Derivatives

The scope of credit derivatives includes total return swaps, credit swaps, and other credit derivatives.

(A) Total Return Swaps Credit derivatives unbundle default risk from the other features of a loan. The original lender no longer needs to bear the risk; it can be transferred to others for a price. The party who wishes to transfer is known as the protection buyer. The protection seller assumes the credit risk and receives a premium for providing this insurance. The premium is based on the probability and likely severity of default.

The protection buyer is assumed to hold a risky debt instrument and agrees to pay out its total return to the protection seller. This return consists of the stream of interest payments together with the change in the instrument's market value. The protection seller agrees to pay some reference rate and perhaps a negative or positive spread from this rate.

(B) Credit Swaps A credit swap, also known as a default swap, is similar in concept to the total return swap but different in the detail. The protection buyer pays a specific premium to the protection seller, insurance against a risky debt instrument deteriorating in quality. The annuity premium is paid each period until the earlier of the maturity of the credit swap agreement or a specific credit event occurring, usually default. If the credit event occurs, the protection seller pays the protection buyer a contingent amount. This often takes the form of physical settlement, where the protection buyer "puts" the defaulted obligation to the protection seller at its face value. The economic cash flow is the difference between the face value of the instrument and its market value. Thus, the protection buyer receives payment only when a specific credit event occurs; otherwise, the cash flow from the protection seller is zero. The periodic premium paid is called the credit swap spread. This cost of protection depends on the credit rating of the company, risk mitigation, and likely recovery should default occur.

(C) Other Credit Derivatives Other credit derivatives include spread adjusted notes, credit options, and credit-sensitive notes.

- **Spread adjusted notes** involve resets based on the spread of a particular grade of security over Treasury securities. An index is specified, and quarterly and semiannual resets occur, where one counterparty must pay the other depending on whether the quality yield spread widens or narrows. Usually the spread is collared with a floor and cap.
- **Credit options** involve puts and calls based on a basket of corporate fixed income securities. The strike price often is a specified amount over Treasury securities.
- With **credit-sensitive notes**, the coupon rate changes with the credit rating of the company involved. If the company is downgraded, the investor receives more interest income; if the company is upgraded, the investor receives less interest income.

DEFINITIONS OF KEY TERMS: CURRENCY AND CREDIT DERIVATIVES

Abandonment options. Options that can be structured so that they provide the option to reduce capacity or temporarily suspend operations.

Basis risk. The difference between two risks or prices.

Call option. An option to buy (call) a share of stock at a certain price within a specific period.

Call swaption. Involves paying floating rate and receiving fixed rate in the swap.

Cap. A put option on a fixed income security's value.

Collar. A combination of a cap and a floor, with variation only in the midrange.

Flexibility options. These permit the firm to alter operations depending on how conditions change during the life of the project.

Floor. A call option.

Growth option. Allows a company to increase its capacity if market conditions are better than expected. Variations of the growth options include increasing the capacity of an existing product line, expanding into new geographic markets, and adding new products.

Interest rate risk. The risk that interest rates will change in an unfavorable direction.

In-the-money option. Occurs when it is beneficial financially for the option holder to exercise the option. A gain will be realized if the option is exercised.

Liquidity risk. Refers to the ability to find a counterparty to enter or terminate a transaction.

Managerial (strategic) options. Give managers a chance to influence the outcomes of a project. These options are used with large and strategic projects.

Market risk. The risk that the value of the agreement will change.

Out-of-the-money option. Occurs when it is not beneficial financially for the option holder to exercise the option. A loss would be incurred if the option is exercised.

Protection buyer. Pays the protection seller to assume the credit risk.

Put option. The option to sell a specified number of shares of stock at a prespecified price during a particular period.

Put swaption. Involves paying a fixed rate and receiving a floating rate in the swap.

Striking price or exercise price. The price that must be paid (buying or selling) for a share of common stock when an option is exercised.

(iv) Hidden Financial Reporting Risks

Off–balance sheet accounting practices include hiding debt with: the equity method, with lease accounting, with pension accounting, and with special-purpose entities. In all these cases, debt

is underreported, which creates a financial reporting risk. Investors and creditors charge a premium for the financial reporting risk. Consequently, the cost of capital goes up and stock prices and bond prices go down.

The equity method hides liabilities because it nets the assets and liabilities of the investee. Since assets are greater than liabilities, this net amount goes on the left-hand side of the balance sheet. This type of accounting practice hides all of the investee's debts.

Use of operating lease accounting "gains" managers an understatement of their firm's financial structure by 10 to 15 percentage points. Footnotes to financial statements can help investors, creditors, and analysts to unravel the truth.

Huge amounts of money are involved in pension accounting. Pension expenses include the service cost plus the interest on the projected benefit obligation minus the expected return on plan assets plus the amortization of various unrecognized items, such as the unrecognized prior service cost. The only item found on the balance sheet is the prepaid pension asset or the accrual pension cost, which in turn equals the pension assets minus the projected benefit obligation minus various unrecognized items. The netting of the projected benefit obligations and the pension assets is incorrect; consequently, investors, creditors, and analysts must "unnet" them to gain a better understanding of the truth. Another area of concern is the assumptions about interest rates and the need to assess their appropriateness.

Special-purpose entity debt includes securitizations and synthetic leases. Securitizations take a pool of homogeneous assets and turn them into securities. The idea is to borrow money from investors, who in turn are repaid by the cash generated by the asset pool. This process includes mortgages, credit card receivables, transportation equipment, energy contracts, water utilities, and trade A/R. Securitizations are big business and represent a financial risk since these amounts are not shown on the balance sheet. Synthetic leases constitute a technique by which firms can assert that they have capital leases for tax purposes but operating leases for financial reporting purposes. They form a way for companies to decrease income taxes without admitting any debt on their balance sheets.

(v) Financial Engineering

The scope of financial engineering involves creating new financial instruments (derivative securities) or combining existing derivatives to accomplish specific hedging goals (e.g., reduce financial risk). A derivative security is a financial asset that represents a claim to another financial asset (e.g., a stock option that gives the owner the right to buy or sell stock). Financial risk may result from changes in domestic and international interest rates, foreign exchange rates, and commodity prices.

Tools for managing financial risk include hedging with: forward contracts, futures contracts, currency option contracts, and currency swap contracts. These tools allow a firm to reduce or even eliminate its exposure to financial risks. Hedging avoids a firm's expensive and troublesome disruptions that result from short-run and temporary price fluctuations. It gives a firm the ability to react and adapt to changing financial market conditions.

Financial engineering can also be applied to insurance and reinsurance areas using captive insurance methods and alternate risk transfer methods as part of a company's risk management and risk mitigation strategy.

(g) Cash Management

(i) Cash Controls

The standard medium of exchange is cash, which provides the basis for measuring and accounting for all other items. To be presented as cash on the balance sheet, it must be available to meet current obligations. Cash includes such items as coins, currency, checks, bank drafts, checks from customers, and money orders. Cash in savings accounts and cash in CDs maturing within one year can be included as current assets, preferably under the caption of short-term investments, but not as cash. Petty cash and other imprest cash accounts can be included in other cash accounts.

Current assets are those assets expected to be converted into cash, sold, or consumed within one year or within the operating cycle, whichever is longer. Current assets are properly presented in the balance sheet in the order of their liquidity. Some of the more common current assets are cash, marketable securities, A/R, inventories, and prepaid items.

(A) Cash Items Excluded The portion of an entity's cash account that is a compensating balance must be segregated and shown as a noncurrent asset if the related borrowings are noncurrent liabilities. If the borrowings are current liabilities, it is acceptable to show the compensating balance as a separately captioned current asset.

RULES FOR COMPENSATED BALANCES

- If related borrowings are noncurrent liabilities, then show the compensated balance as a noncurrent asset.
- If related borrowings are current liabilities, then show the compensated balance as a current asset.

Certain cash items are not presented in the general cash section of the balance sheet. They include compensating balances, other restricted cash, and exclusions from cash.

Compensating Balances The SEC defines compensating balances as "that portion of any demand deposit (or any time deposit or certificate of deposit) maintained by a corporation which constitutes support for existing borrowing arrangements of the corporation with a lending institution. Such arrangements would include both outstanding borrowing and the assurance of future credit availability."

The classification of compensating balances on the balance sheet depends on whether the compensation relates to short-term or long-term borrowing. If held for short-term borrowing, it should be presented separately in current assets. If held for long-term borrowing, it should be classified as a noncurrent asset under investments or other assets.

Where compensating balance arrangements exist but do not legally restrict the use of cash, the arrangements and amounts should be disclosed in the footnotes of the financial statements.

Other Restricted Cash Cash balances can be restricted for special purposes, such as dividend payments, acquisition of fixed assets, retirement of debt, plant expansion, or deposits made in connection with contracts or bids. Since these cash balances are not immediately available for

just any use, they should be presented separately in the balance sheet. Classification as current or noncurrent is dependent on the date of availability or disbursement.

Exclusions from Cash Items that should not be presented as cash are postage stamps, postdated checks, travel advances, IOUs, securities, investments in federal funds, and checks deposited and returned because of insufficient funds. CDs should be reflected in the temporary investment account, since they are not available for use until the maturity date.

As mentioned earlier, cash includes coins and currency on hand and demand deposits available without restrictions. Cash in a demand deposit account that is being held for the retirement of long-term debts not maturing currently should not be included in the current assets. Instead, it should be shown as a noncurrent investment. The key criterion is management's intention that the cash be available for current purposes. Cash equivalents include other forms of near cash as well as demand deposits and liquid, short-term securities. *The key point is that the cash equivalents must be available on demand similar to cash.*

SUGGESTED DISCLOSURES FOR CASH

- Amount and nature of restricted cash
- Amount and nature of compensating balances
- Overdrafts presented as current liabilities

(B) Bank Reconciliation Every organization should prepare a bank reconciliation schedule periodically (e.g., monthly) to reconcile the organization's cash record with the bank's record of the organization's cash. It is unusual for these two sets of records to be the same due to errors and timing differences, such as

- Bank or depositor (customer) errors
- Bank credits
- Bank charges
- Deposits in transit
- Outstanding checks

A widely used method reconciles both the bank balance and the book balance to a correct cash balance. This is shown in Exhibit 7.20.

Cash requires a good system of internal control, since it is so liquid and easy to conceal and transport. Segregation of duties is an important part of the system of internal control for cash. No one person should both record a transaction and have custody of the asset. Without proper segregation, it is easier for an employee to engage in lapping. **Lapping** is a type of fraud in which an employee misappropriates receipts from customers and covers the shortages in these customers' accounts with receipts from subsequent customers. Therefore, the shortage is never eliminated but rather is transferred to other accounts. Lapping schemes do not require employees to divert funds for personal use. The funds can be diverted for other business expenses.

Balance per bank statement	
Add:	Deposits in transit
	Undeposited cash receipts
	Bank errors (understating the bank balance)
Deduct:	Outstanding checks
	Bank errors (overstating the bank balance)
Correct cash balance (item 1)	
Balance per depositor's books	
Add:	Bank credits and collections not yet recorded in the books
	Book errors (understating the book balance)
Deduct:	Bank charges not yet recorded in the books
	Book errors (overstating the book balance)
Correct cash balance (item 2)	

The goal is to make item 1 and item 2 equal.

EXHIBIT 7.20 Reconciliation of Bank Balance with Book Balance

Kiting is a scheme in which a depositor with accounts in two or more banks takes advantage of the time required for checks to clear in order to obtain unauthorized credit. The scheme would not exist if depositors were not allowed to draw against uncollected funds. The use of uncollected funds does not always indicate a kite; such use can be authorized by an officer of the bank. Kiting schemes can be as simple as cashing checks a few days before payday, then depositing the funds to cover checks previously written. Or, they can be as complex as a systematic buildup of uncollected deposits, pyramiding for the "big hit." Kiting can be eliminated or reduced through electronic funds transfer (EFT) systems. Kiting can be detected when reviewing accounts to determine if a customer or employee is drawing a check against an account in which he or she has deposited another check that has not yet cleared.

Float is an amount of money represented by items (both check and noncheck) outstanding and in the process of collection. The amount of float incurred is determined by two factors: the dollar volume of checks cleared and the speed with which the checks are cleared. The relationship between float and these two factors can be expressed as

$$\text{Float} = \text{Dollar volume} \times \text{Collection speed}$$

The cost of float pertains to the potential for earning income from nonearning assets, as represented by items in the process of collection. This cost of float is an opportunity cost—the firm could have fully invested and earned income had the funds been available for investment and not incurred float.

In a financial futures **hedging** transaction, a firm takes a futures position that is opposite to its existing economic or, to use the more commonly name, "cash" position. By taking the opposite position in the financial futures market, the firm can protect itself against adverse interest rate fluctuations by locking in a given yield or interest rate.

(ii) Controls over Cash

Cash is a precious resource in any organization. Cash is required to pay employee wages and salaries, buy raw materials and parts to produce finished goods, pay off debt, and pay dividends,

among other things. Cash is received from customers for the sale of goods and the rendering of services. Customer payments come into the organization in various forms, such as checks, bank drafts, wire transfers, money orders, charge cards, and lockbox systems. The cash manager's primary job is to ensure that all customer payments funnel into the company's checking accounts as fast as possible with greater accuracy. Payments received at lockboxes located at regional banks flow into cash concentration accounts, preferably on the same day of deposit.

The cash manager should focus on reducing the elapsed time from customer payment date to the day funds are available for use in the company's bank account. This elapsed time is called the "float."

A major objective of the cash manager is to accelerate the cash inflow and slow the cash outflow without damaging the company's reputation in the industry. To do this, the cash manager needs to find ways to accelerate cash flows into the company, which, in turn, reduce investment in working capital. Similarly, the cash manager needs to find ways to slow the outflow of cash by increasing the time for payments to clear the bank. Another major objective is not to allow funds sitting idle without earning interest.

The cash manager needs to focus on seven major areas for effective cash management (See Exhibit 7.21):

1. Cash account balances
2. Purchases
3. Payables
4. Manufacturing
5. Sales
6. Receivables
7. Lockbox systems

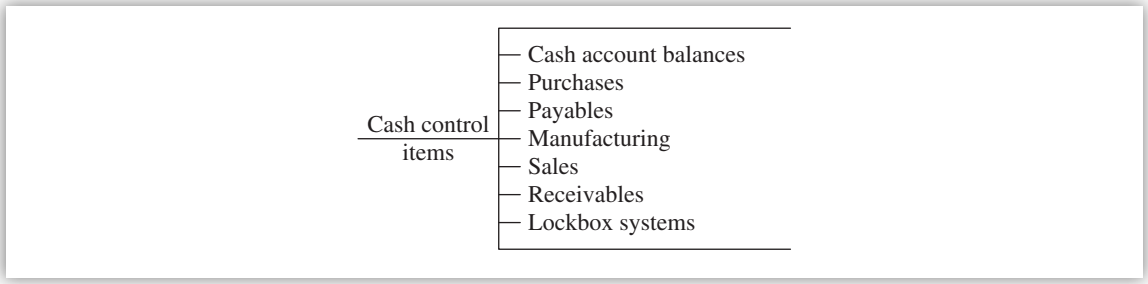


EXHIBIT 7.21 Cash Control Items

(A) Cash Account Balances The following actions are advised to strengthen controls in cash accounts:

- Take an inventory of cash accounts open. Since each account maintains cash balances, the potential exists to improve control over cash.
- Perform account reconciliations periodically, and ensure that the person doing the reconciliation has no cash management duties.
- Review the account of compensating balances held at the banks. Focus on eliminating or reducing the amount of compensating balances.

- Review cash account balances to see if they are kept too high for fear of being overdrawn. Try to bring these balances down to the bare minimum without being overdrawn. Doing this will improve the idle cash situation.
- Review the fees charged by the bank for the number of accounts open, and understand the reasons for the service fees charged.

CASH CONTROLS

The more accounts there are, the fewer the controls are over cash balances. Consequently, there is a higher likelihood that there will be significant idle funds sitting in those accounts.

(B) Purchases The method of payment and the payment date can impact the firm's cash situation. An early payment date demanded by a vendor could add to the interest expense. Payment discounts should be taken by making payment within a specified time. The cash manager should review any purchase contracts containing clauses with unusual late fees and interest rates on unpaid balances.

(C) Payables The following actions are advised to strengthen controls in payables:

- Establish policies concerning the average payment period. The payment period is calculated by dividing the A/P balance by the average daily credit purchases.
- Use remote disbursement banks, preferably with zero balance.
- Perform periodic aging of the A/P.

(D) Manufacturing The following actions are advised to strengthen controls in manufacturing:

- Be aware of labor union contract negotiations since their outcome will affect cash balances.
- Be aware of the sale of obsolete or overstocked inventory that will suddenly increase the inflow of cash that must be put to work (i.e., invested).

(E) Sales Credit policies should be balanced. Overly lenient credit policies will cause a rise in payment delinquencies and bad debt, which will create a funding gap in the cash position.

- If bad debts are increasing due to lenient credit policies, see if the sales force commission payment policy can be changed from a gross sales basis to a collected balances basis.
- If credit policies are overly stringent, the firm will lose its customers to competition.

(F) Receivables The following actions are advised to strengthen controls in receivables:

- Review billing and collection policies and procedures.
- Minimize the elapsed time between sale and release of invoice to the customer.
- Reduce the long time between invoice preparation and entry of the invoice into the receivables system.
- Identify receivable backlogs, and determine their impact on cash position.

- Minimize the time required to record the payment and to remove it from the receivable subledger. If the time lag is too long, collection resources will be wasted pursuing accounts that have already paid.
- Perform aging of receivables.
- Establish procedures related to the types of collection efforts, including customer statements, dunning letters, phone calls by trained in-house staff, referral to a collection agency, and so forth.
- Establish policies toward selling the receivables or clarify the policies toward using the receivables as collateral for financing purposes.

(G) Lockbox Systems Most banks offer both retail and wholesale lockbox services. Wholesale lockboxes collect payments from other companies; here the volume of transactions is small and the dollar amount of each transaction is large. Retail lockboxes receive payments from individual customers; here the volume of transactions is large and the dollar amount of each transaction is small.

SELECTION CRITERIA FOR LOCKBOX BANKS

If the company has customers scattered around the country and payments are all sent to a single centralized location, use of a lockbox is advisable. Banks servicing the lockboxes are chosen for their proximity to the lockbox, their processing capability, their ability to transfer funds quickly to the cash concentration system, and geographic concentration of customers.

With the lockbox systems, most of the float has been squeezed from the cash management systems of both vendor and customer. These cash acceleration techniques have been referred to as a zero-sum game with no advantage for either side of the transaction (i.e., vendor and customer). Lockbox systems help sellers stay even with their customers in the race to accelerate cash inflow and delay its outflow. *Elimination of float accelerates cash inflow.*

Two types of lockbox systems are in use: manual and electronic. The **manual lockbox** system collects and processes the checks and deposits them into the customer's account. Then the bank sends the money to the cash concentration account and sends the payment information to the customer via a magnetic tape or telecommunication transmission for entry into the A/R system. The funds are transferred from the lockbox account to the cash concentration account through the use of depository transfer checks, wire transfers, or ETFs through an automated clearinghouse.

Electronic lockboxes eliminate checks and automate the transfer payment data from company to company as a wholesale transaction. When a customer receives a vendor's invoice, the customer calls the third-party computer to make payment. The third party can be a bank or a service bureau, which acts as a payment collector. After the daily cutoff, the payment collector transmits the daily payment receipts file to the vendor's computer for automatic processing by the vendor's A/R system.

Some **advantages** of an electronic lockbox system are listed next.

- Cash inflow accelerates because there is no float.

- Misapplied and partial payments do not exist since the payment collector does not accept partial payment, and the customer account is verified prior to payment entry applied properly.
- Information about nonsufficient funds comes back faster than for returned checks.
- Credit controls can be tightened for high-risk or slow-paying customers.
- It reduces the days of sales outstanding ratio, which measures the velocity of collections.

Disadvantages of an electronic lockbox system are the high initial system design cost and cost per transaction and service fees by the third-party payment collector.

(iii) Electronic Techniques to Control Cash

In addition to the electronic lockboxes just discussed, two other electronic techniques to control cash need to be mentioned. These include EFT and electronic data interchange (EDI) systems.

(A) Electronic Funds Transfer EFT systems allow organizations to pay their bills without actually writing checks. EFT eliminates bank float as "good" funds move quickly from customer accounts to vendor accounts at their respective banks. EFT accelerates cash inflow for the company receiving payment.

The EFT system removes several days from the entire payment cycle of cutting a paper check, mailing it, depositing it, clearing it through the bank, recording its payment in the customer's A/P system, and recording the cash receipts in the vendor's A/R system. The only cycle time is the time for physically receiving the goods or services through truck, car, by rail, or other.

The automated clearinghouse (ACH) clears debits and credits created by ETFs. The ACH clears all transactions each day by properly debiting and crediting them to the correct accounts. The ACH then routes these cleared transactions to the proper member banks.

(B) Electronic Data Interchange The EDI system is another major step towards a payment acceleration scheme. EDI is used not only to place purchase orders with vendors for raw materials and finished goods but also to send invoices and receive payments. The EDI system automatically creates the invoice and sends it to the customer. After receiving the goods, the customer authorizes an electronic payment with virtually no float. EDI involves a third party as a middleman to transmit and receive electronic messages between vendors and customers.

The data transferred between vendor and customer contain this information:

- Dollar amount
- Invoice number
- Purchase order number
- Customer number
- Discounts taken
- Shipping instructions
- Product delivery dates
- Payment due dates

Electronic payments are posted automatically to the vendor's A/R system. A major **advantage** of EDI is that the posting is fast, not subject to human errors, and it accelerates cash inflows. A major **drawback** of the EDI system is the need to have a standardized format of data transmitted between vendors and customers. This could limit the flexibility of doing business with many parties.

(iv) Management of Current Assets

Effective cash management requires a working capital policy, which refers to the firm's policies regarding the desired level for each category of current assets and how current assets will be financed. The components of current assets in order of liquidity are shown in Exhibit 7.22.

Cash (most liquid)
Marketable securities
Accounts receivable
Prepaid expenses
Inventories (least liquid)

EXHIBIT 7.22 Components of Current Assets

Current assets fluctuate with sales and represent a large portion (usually greater than 40%) of total assets. Working capital management is important for large and small firms alike.

DEFINITIONS OF KEY TERMS: WORKING CAPITAL

Net working capital means current assets minus current liabilities.

Working capital or **gross working capital** means current assets.

Working capital management involves the administration of current assets and current liabilities.

For financing current assets, most small firms rely on trade credit and short-term bank loans, both of which affect working capital by increasing current liabilities. A/P represents "free" trade credit when discounts are taken. This is similar to an interest-free loan. However, current liabilities are used to finance current assets and in part represent current maturities of long-term debt. Large firms usually rely on long-term capital markets, such as stocks. The components of current liabilities are shown in Exhibit 7.23 with their associated costs.

Accounts payable (free trade credit)
Accrued wages
Accrued taxes
Notes payable (not free)
Current maturities of long-term debt

EXHIBIT 7.23 Components of Current Liabilities

The relationship between sales and the need to invest in current assets is direct, as shown in the next examples: As sales increase, A/R increases, inventory will increase, and cash needs increase. Any increase in an account on the left-hand side of the balance sheet must be matched by an increase on the right-hand side. It involves matching maturities of assets and liabilities. That is, current assets are financed with current liabilities, and fixed assets are financed with long-term debt or stock. This is done to reduce interest rate risk.

Example Computation of Changes in Cash and Net Working Capital

Example 1

Partial balance sheet information for a company for the years ending December 31, 20X1 and 20X2 is shown next.

	December 31	
	20X1	20X2
Current assets (except for cash):		
Accounts receivable	$20,000	$ 5,000
Inventories	50,000	14,000
Prepaid expenses	3,000	6,000
Current liabilities:		
Accounts payable	32,000	16,000
Property tax payable	4,000	3,000

Working capital (WC) is assumed to increase in 20X2 by $12,000.

Question: What is the change in cash in 20X2?

Answer: The change is –$19,000, as shown next, where CA refers to capital assets, CL refers to capital liabilities and Δ refers to change

$$\begin{aligned}\Delta\text{Cash} &= \Delta\text{WC} - \Delta\text{Noncash CA} + \Delta\text{CL}\\ &= 12{,}000 - (15{,}000 + 36{,}000 - 3{,}000)\\ &\quad + (16{,}000 + 1{,}000)\\ &= -19{,}000\end{aligned}$$

Example 2

The next amounts pertain to the ABC Corporation at December 31, 20X2.

Total current assets	$ 300,000
Total fixed assets	2,200,000
Total assets	2,500,000
Total current liabilities	120,000
Total liabilities	1,600,000
Total paid-in capital	400,000
Total stockholders' equity	900,000

Question: What is the ABC's net working capital at December 31, 20X2?

Answer: It is $180,000. Net working capital is computed by subtracting total current liabilities ($120,000) from total current assets ($300,000), which in this case yields an answer of $180,000.

(A) Cash Conversion Cycle Model The cash conversion model defines the length of time from the payment for the purchase of raw materials to the collection of A/R generated by the sale of the final product. It is an important model since it focuses on the conversion of materials and labor to cash. The model is represented in Exhibit 7.24.

Cash conversion cycle	=	Inventory conversion period (1)	+	Receivables conversion period (2)	−	Payables deferral period (3)

where:
(1) Inventory conversion period = Length of time required to convert raw materials into finished goods and then to sell those goods
(2) Receivables conversion period = Length of time required to convert the firm's receivables into cash
(3) Payables deferral period = Average length of time between the purchase of raw material and labor and the payment of cash for them

EXHIBIT 7.24 Cash Conversion Model

The cash conversion cycle begins the day a bill for labor and/or supplies is paid and runs to the day receivables are collected. The cycle measures the length of time the firm has funds tied up in working capital. The shorter the cash conversion cycle, the smaller the need for external financing and thus the lower the cost of such financing. This would result in increase in profits.

Example Calculation of Cash Conversion Cycle

It takes a firm 70 days from the purchase of raw materials to the sale of finished goods, 50 days after a sale to convert a receivable into cash, and 30 days to pay for labor and materials. The firm's cash conversion cycle is 90 days, as shown next.

70 days + 50 days – 30 days = 90 days or

(Delay in receipt of cash) – (Payment delay) = Net delay

The firm needs to finance the costs of processing for a 90-day period. Its goals should be to shorten its cash conversion cycle without jeopardizing business operations, (i.e., without increasing costs or decreasing sales).

(B) Approaches to Shorten the Cash Conversion Cycle The next list presents ways to shorten the cash conversion cycle:

- Reduce the inventory conversion period by processing and selling goods more quickly.
- Reduce the receivables conversion period or days sales outstanding by speeding up collections.
- Lengthen the payables deferral period by slowing down payments.

(C) Working Capital Asset Investment Policies Appropriate working capital policies are needed to support various levels of sales. Three such policies include relaxed, moderate, and restricted (see Exhibit 7.25).

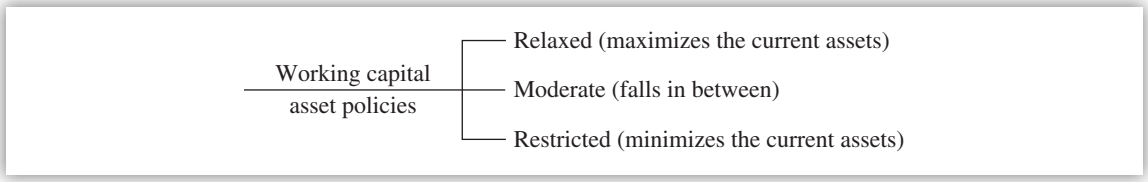


EXHIBIT 7.25 Working Capital Asset Policies

- **Relaxed (liberal) working capital policy.** Sales are stimulated by the use of a credit policy that provides liberal financing to customers, which results in a high level of A/R. This policy maximizes current assets. A/R will increase as credit sales increase for a relaxed policy; the opposite is true for the restricted policy.
- **Moderate working capital policy.** This policy falls between liberal and tight working capital policy.
- **Restricted (tight) working capital policy.** This policy minimizes current assets. A tight policy lowers the receivables for any given level of sales or even the risk of a decline in sales. This policy provides the highest expected return on investment and entails the greatest risk. The firm would hold minimal levels of safety stocks for cash and inventories.

CERTAINTY VERSUS UNCERTAINTY OF BUSINESS CONDITIONS

- Under conditions of certainty, the firm knows the sales, costs, order lead times, and collection periods. All firms would hold the same level of current assets. Any larger amounts would increase the need for external funding without a corresponding increase in profits. Any decrease in amounts would involve late payments to suppliers, lost sales, and production inefficiencies because of inventory shortages.
- Under conditions of uncertainty, the firm does not know the sales, costs, order lead times, and collection periods. The firm requires some minimum amount of cash and inventories based on expected payments, sales, safety stocks, and order lead times. Safety stocks help deal with deviations of sales from expected values.

(D) Working Capital Financing Policies A good working capital financing policy is needed to handle seasonal or cyclical business fluctuations and a strong or weak economy. When the economy is strong, working capital is built up and inventories and receivables go up. When the economy is weak, working capital goes down along with inventories and receivables. Current assets are divided into permanent and temporary, and the manner in which these assets are financed constitutes the firm's working capital financing policy.

A firm's working capital asset policy, including its cash conversion cycle, is always established in conjunction with the firm's working capital financing policy. Three financing policies are available to manage working capital: maturity matching, an aggressive approach, and a conservative approach.

Example Calculation of Total Assets

	January 1 (million)	June 30 (million)
Cash and marketable securities	4	4
Accounts receivable	6	8
Inventories	15	20
Current assets	25 (1)	32 (2)
Fixed assets	40	40
Total assets	65	72

(1) Permanent current assets that are still on hand at the trough of a firm's cycles.

(2) Temporary assets that fluctuate with seasonal or cyclical sales variation that fluctuates from zero to a maximum of $7 million (i.e., 32 – 25 = 7).

The maturity matching, or self-liquidating, approach requires that asset maturities are matched with liability maturities. This means permanent assets are financed with long-term capital to reduce risk. Each loan would be paid off with cash flows generated by assets financed by the loan, so loans would be self-liquidating. Uncertainty about the lives of assets prevents exact matching in an *ex post* sense.

MATURITY MATCHING—ASSETS VERSUS DEBT

- If long-term assets are financed with short-term debt, there might be a problem in making the required loan payments if cash inflows are not sufficient. The loan may not be renewed.
- If long-term assets are financed with long-term debt, the required loan payments would have been matched with cash flows from profits and depreciation. No question of loan renewals will come up.

Characteristics of aggressive approach to maturity matching	Characteristics of conservative approach to maturity matching
Financing of part of permanent current assets is accomplished with short-term credit.	Financing of all permanent assets is accomplished with long-term capital.
Financing of all current assets and part of fixed assets is accomplished with short-term credit.	The firm uses a small amount of short-term credit to meet its peak requirements.
Financing of all current assets and part of fixed assets is accomplished with short-term credit.	The length of the cash conversion cycle is longer because higher levels of inventories and receivables lengthen the inventory and receivables conversion periods.
There is a trade-off between safety and profits since short-term debt is cheaper than long-term debt.	
The length of the cash conversion cycle is shorter since the firm holds a minimal level of cash, securities, inventories, and receivables. Inventories and receivables conversion periods would be shorter.	

EXHIBIT 7.26 Characteristics of Aggressive and Conservative Approaches to Maturity Matching

Two approaches are used in maturity matching: the aggressive (nonconservative) approach and the conservative approach. Exhibit 7.26 presents characteristics of these two approaches.

(E) Advantages and Disadvantages of Short-Term Credit Short-term credit is generally riskier and cheaper than using long-term credit. There is a trade-off between risk and profits in using short-term credit. The three financing policies discussed earler differ in the relative amount of short-term debt financing each uses, as shown in Exhibit 7.27.

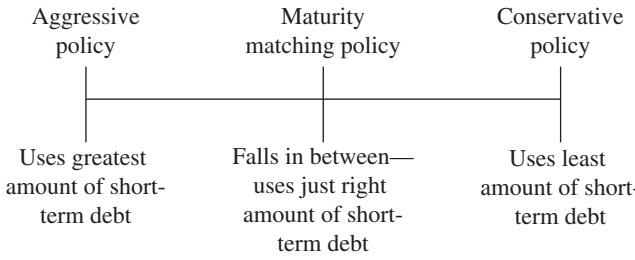


EXHIBIT 7.27 Debt Financing with Short-Term Credit

Although short-term credit has disadvantages, it also has some advantages, as shown in exhibit 7.27.

(F) Management of Cash On one hand, adequate cash serves as protection against a weak economy and can be used to pay off debts and to acquire companies. On the other hand, too much cash makes a firm vulnerable to corporate raiding or takeovers.

$$\text{Cash} = \text{Currency} + \text{Bank demand deposits} + \text{Near-cash marketable securities}$$

$$\text{Near-cash marketable securities} = \text{U.S. Treasury bills} + \text{Bank CDs}$$

Effective cash management is important to all organizations, whether profit oriented or not. The scope of cash management encompasses cash gathering (collection) and disbursement techniques and investment of cash. Since cash is a "nonearning" asset until it is put to use, the goal of cash management is to reduce cash holdings to the minimum necessary to conduct normal business. See Exhibit 7.28 for advantages and disadvantages of short-term and long-term credit.

EXHIBIT 7.28 Advantages and Disadvantages of Short-Term and Long-Term Credit

Advantages and disadvantages of short-term credit	Advantages and disadvantages of long-term credit
Advantages	**Advantages**
A short-term loan can be obtained much more quickly than a long-term loan.	Interest costs are fixed and stable over time.
A short-term loan can accommodate seasonal or cyclical needs for funds.	Long-term debt is subject to less risk than short-term debt.
It provides flexible repayment schedules.	Temporary changes in either the general level of interest rates or the firm's own financial position do not adversely affect long-term debt.
It has less restrictive provisions.	Long-run performance can overcome short-run recession.
Interest rates are generally lower than on long-term debt due to upward sloping of the yield curve.	

Financing is less expensive than long-term debt.	
Net income and the rate of return on equity will be higher than on long-term debt due to lower interest rates for short-term debt.	
Disadvantages	**Disadvantages**
Short-term debt is subject to more risk (interest-rate risk) than long-term debt due to fluctuating interest expense and the possibility of bankruptcy.	Lenders will require thorough financial examination before granting a long-term loan, which takes time for approval.
It runs the risk of having to refinance the short-term debt at a higher interest rate, which would lower the rate of return on equity.	Long-term loans require a detailed loan agreement.
There is the possibility of being unable to renew the debt when its loans mature, thus of facing maturity risk. Also, tight money supply, labor problems, extreme competition, low demand for products, and higher interest rates will make creditors raise interest rates.	Flotation costs are higher.
	Prepayment penalties can be expensive.
	Long-term loans can contain provisions or covenants that may constrain the firm's future actions.
	Interest rates are higher than on short-term debt due to downward sloping of the yield curve.

There are four reasons for holding cash by organizations, as shown in Exhibit 7.29.

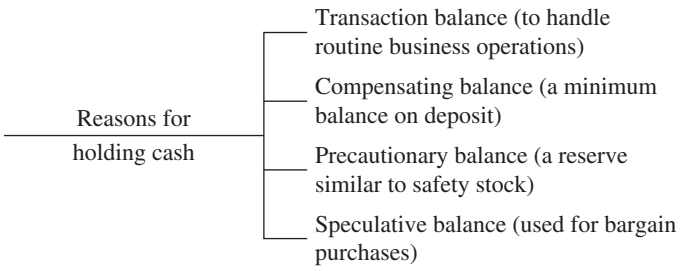


EXHIBIT 7.29 Reasons for Holding Cash

1. **Transaction balance.** Payments and collections are handled through the cash account. These routine transactions are necessary in business operations.
2. **Compensating balance.** A bank requires the customer to leave a minimum balance on deposit to help offset the costs of providing the banking services. The balance is compensation paid to banks for providing loans and services. Some loan agreements also require compensating balances.

3. **Precautionary balance.** Firms hold some cash in reserve to accommodate for random, unforeseen fluctuations in cash inflows and outflows. These are similar to the safety stocks used in inventories.

KEY CONCEPTS TO REMEMBER: Management of Cash

- The less predictable the firm's cash flows, the longer the need for a precautionary balance, and vice versa. The easier the access to borrowed funds on short notice, the lower the need to hold cash for precautionary purposes, and vice versa.
- Marketable securities can be an attractive alternative to holding cash for precautionary purposes since they can provide greater interest income than cash.

4. **Speculative balance.** Cash may be held to enable the firm to take advantage of any bargain purchases that might arise. Similar to precautionary balances, firms could rely on reserve borrowing capacity and on marketable securities rather than on cash for speculative purposes.

A total desired cash balance for a firm is not simply the sum of cash in transaction, compensating, precautionary, and speculative balances. This is because the same money often serves more than one purpose. For example, precautionary and speculative balances can also be used to satisfy compensating balance requirements. A firm needs to consider these four factors when establishing its target cash position.

(G) Advantages of Holding Adequate Cash and Near-Cash Assets In addition to the motives for transaction, compensating, precautionary, and speculative balances, there exist other reasons for firms to hold adequate cash and near-cash assets. These advantages are listed next.

- Taking trade discounts. Suppliers offer customers trade discounts—discounts for prompt payment of bills. Cash is needed to take advantage of trade discounts. The cost of not taking trade discounts could be high.
- Keeping current ratios and acid-test ratios in line with those of other firms in the industry requires adequate holdings of cash. Higher ratios give a strong credit rating. A strong credit rating enables the firm to purchase goods and services from suppliers and provide favorable terms and to maintain an ample line of credit with the bank. A weak credit rating does the opposite.
- Holding an ample supply of cash could help a firm to acquire another firm, to handle contingencies such as labor strikes, to attack competitors' marketing campaigns, and to take advantages of special offers by suppliers.

(H) Cash Management Efficiency Techniques A cash budget, showing cash inflows and outflows and cash status, is the starting point in the cash management system. The techniques used to increase the efficiency of management are listed next.

- Cash flow synchronization
- Use of float

- Speeding collections
- Slowing disbursements
- Transfer mechanisms

These techniques are shown in Exhibit 7.30.

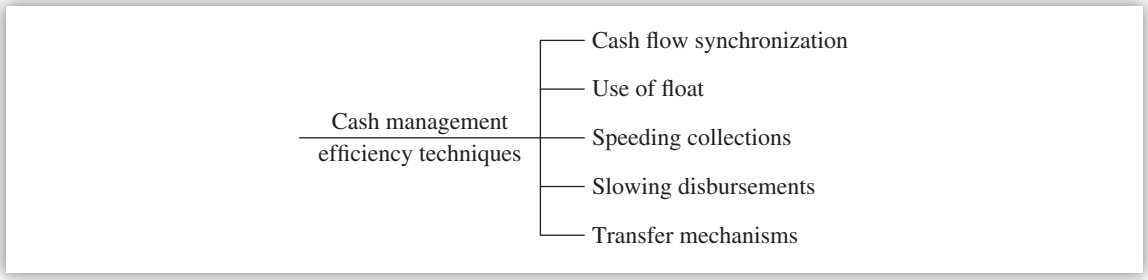


EXHIBIT 7.30 Cash Management Efficiency Techniques

Cash Flow Synchronization When cash inflows coincide with cash outflows, the need for transaction balances will be low. The benefits would be to reduce cash balances, decrease bank loan needs, reduce interest expenses, and increase profits.

Use of Float Two kinds of float exist: disbursement float and collection float. The difference is net float. Disbursement float arises when one makes a payment by a check. It is defined as the amount of checks that one has written but are still being processed and thus have not yet been deducted from the checking account balances by the bank. Collection float arises when one receives a check for payment. It is defined as the amount of checks that have been received but that are in the collection process. It takes time to deposit the check, for the bank to process it, and to credit an account for the amount collected.

$$\text{Net float} = \text{Disbursement float} - \text{Collection float}$$
$$\text{Net float} = \text{One's checkbook balance} - \text{Bank's book balance}$$

A positive net float is better than a negative net float because the positive net float collects checks written to a firm faster than clearing checks written to others. Net float is a function of the ability to speed up collections on checks received and to slow down collections on checks written. The key is to put the funds received to work faster and to stretch payments longer.

Speeding Collections Funds are available to the receiving firm only after the check-clearing process has been completed satisfactorily. There is a time delay between a firm processing its incoming checks and in making use of them. Three parties are involved in the check-clearing process: the payer, payee, and the Federal Reserve System (requires a maximum of two days to clear a check). Traditionally, the length of time required for checks to clear is a function of the distance between the payer's and the payee's banks. This has improved significantly due to information technology (IT). The greater the distance, the longer the delay due to regular mail, especially for remote locations. If the payer's and the payee's bank are the same, there is less delay than if they are different.

KEY CONCEPTS TO REMEMBER: Techniques to Speed up Collections

- Lockboxes are used to reduce mail delays and check-clearing delays. Both mail and check collection times are reduced using lockboxes. Lockboxes are mailboxes at the post office.
- Preauthorized debt (checkless transactions) allows funds to be automatically transferred from a customer's account to the firm's account on specified dates. Both mail and check-clearing times are eliminated. Examples include payroll checks, mortgage payments, tax bills, utility bills. The acceptance of a preauthorized debt system by customers is low due to loss of disbursement float and lack of canceled checks as receipt.
- Use of debit cards. Acceptance of debit cards is also low, but predictions are it will pick up in the future.

Slowing Disbursements Three techniques are available to slow down disbursements: delaying payments, writing checks on banks in different locations, and using drafts. Delaying payments has negative consequences, such as a bad credit rating. Customers can sue firms for writing checks on banks in distant locations—playing West Coast banks against East Coast banks in the United States. Speeding the collection process and slowing down disbursements have the same objectives. Both keep cash on hand for longer periods.

Use of drafts seems normal. A check is payable on demand while a draft is not. A draft must be transmitted to the issuer, who approves it and then deposits funds to cover it, after which it can be collected.

Transfer Mechanisms A transfer mechanism is a system for moving funds among accounts at different banks. Three types of transfer mechanisms are depository transfer checks, wire transfers, and electronic depository transfer checks. Each is described next.

- **Depository transfer check (DTC).** Such a check is restricted for deposit into a particular account at a particular bank. A DTC is payable only to the bank of deposit for credit to the firm's specific account. DTCs provide a means of moving money from local depository banks to regional concentration banks and to the firm's primary bank, as shown in Exhibit 7.31.

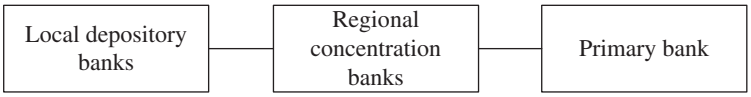


EXHIBIT 7.31 Movement of Depository Transfer Checks

- **Wire transfer.** A wire transfer is the electronic transfer of funds via a telecommunications network that makes funds collected at one bank immediately available from another bank. The wire transfer eliminates transit float and reduces the required level of transaction and precautionary cash balances.
- **Electronic depository transfer check (EDTC).** EDTC is a combination of a wire transfer and a DTC. It provides one-day availability in check clearing time because it avoids the use

of the mail. EDTC is a paperless transaction. EDTC is also called automated clearinghouse (ACH), which is a telecommunication network that provides an electronic means of sending data from one financial institution to another. Magnetic tape files are processed by the ACH, and direct computer-to-computer links are also available.

(v) Management of Marketable Securities

Two basic reasons for holding marketable securities (e.g., U.S. Treasury bills, commercial paper, and CDs) are that they are used as a temporary investment and they serve as a substitute for cash balances. Temporary investment occurs in these cases: The firm must finance seasonal or cyclical operations; the firm must meet some known financial requirements, such as new plant construction program, a bond about to mature, or quarterly tax payments; and when the firm uses proceeds from stocks and bonds to pay for operating assets.

Actually, the choice is between taking out short-term loans or holding marketable securities. There is a trade-off between risks and return. Similar to cash management policy, a firm's marketable security policy should be an integral part of its overall working capital policy. The policy may be a conservative, an aggressive, or a moderate working capital financing policy (see Exhibit 7.32).

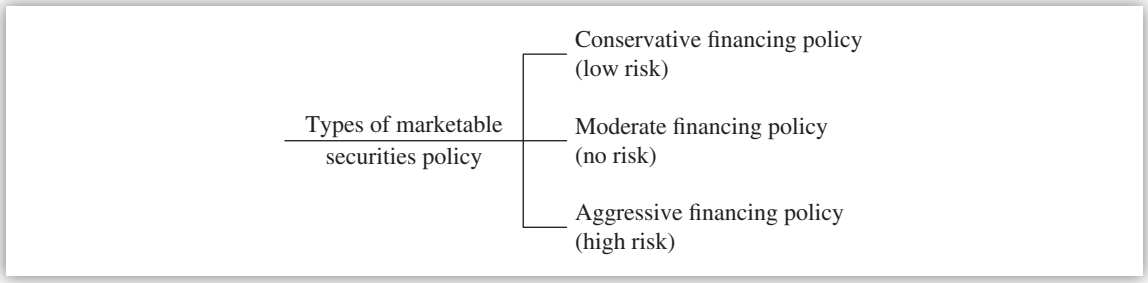


EXHIBIT 7.32 Types of Marketable Securities Policy

- If the firm has a **conservative working capital financing policy**, its long-term capital will exceed its permanent assets, and it will hold marketable securities when inventories and receivables are low. This policy is less risky than the others. There is no liquidity problem since the firm has no short-term debt. However, the firm incurs higher interest rates when borrowing than the return it receives from marketable securities. It is evident that a less risky strategy costs more.
- If the firm has a **moderate working capital financing policy**, the firm will match permanent assets with long-term financing and meet most seasonal increases in inventories and receivables with short-term loans. The firm also carries marketable securities at certain times. With this policy, asset maturities are matched with those of liabilities. No risk exists, at least theoretically.
- If the firm has an **aggressive working capital financing policy**, it will never carry any securities and will borrow heavily to meet peak needs. This is the riskiest method, and the firm will face difficulties in borrowing new funds or repaying the loan, due to its low current ratio. The expected rate of return on both total assets and equity will be higher.

(A) Criteria for Selecting Marketable Securities The selection criteria for a marketable security portfolio include default risk, taxability, and relative yields. The financial manager has several choices available in selecting a marketable securities portfolio, and they all differ in risk and return. Most financial managers are averse to risk and unwilling to sacrifice safety for higher rates of return. The higher a security's risk, the higher its expected and required return, and vice versa. A trade-off exists between risk and return.

Exhibit 7.33 presents the types of marketable securities that are available to financial managers for investment of surplus cash.

Securities suitable to hold as near-cash reserve	Securities not suitable to hold as near-cash reserve
Treasury bills	U.S. Treasury notes and bonds
Commercial paper	Corporate bonds
Negotiable certificates of deposit (CDs)	Common stock and preferred stock
Money market mutual funds	State and local government bonds
Eurodollar time deposits	All of the above with more than one year maturity
All of the above with less than one year maturity	

EXHIBIT 7.33 Marketable Securities Available for Investment of Surplus Cash

Large corporations tend to make direct purchases of U.S. Treasury bills, commercial paper, CDs, and Eurodollar time deposits. Small corporations are more likely to use money market mutual funds as near-cash reserves (because they can be quickly and easily converted to cash). Interest rates on money market mutual funds are lower and net returns are higher than on Treasury bills.

(B) Risks in Marketable Securities Here we review the different types of risk (i.e., default risk, interest rate risk, purchasing power risk, and liquidity risk) facing financial managers in managing the portfolio of marketable securities (see Exhibit 7.34).

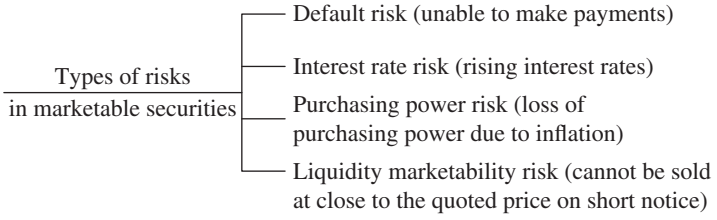


EXHIBIT 7.34 Risks in Marketable Securities

Default Risk The risk that a borrower will be unable to make interest payments or to repay the principal amount upon maturity is known as default risk. For example, the default risk for securities issued by the U.S. Treasury is negligible while securities issued by a corporation and others have some degree of default risk.

The higher the earning power of a firm, the lower its default risk, and vice versa.

Interest Rate Risk The risk to which investors are exposed due to rising interest rates is known as interest rate risk. Interest rate fluctuations are what cause interest rate risk. Even U.S. Treasury bonds are subject to interest rate risk.

Bond prices vary with changes in interest rates. Long-term bonds have more interest rate risk. Short-term bonds have less interest rate risk.

Purchasing Power Risk The risk that inflation will reduce the purchasing power of a given sum of money is known as purchasing power risk. Purchasing power risk is lower on assets whose returns tend to rise during inflation. Purchasing power risk is higher on assets whose returns are fixed during inflation. It is the variability of returns during inflation that determines the purchasing power risk.

Real estate, short-term debt, and common stocks are better hedges against inflation. Bonds and other long-term fixed income securities are not better hedges against inflation.

Liquidity (Marketability) Risk The risk that securities cannot be sold at close to the quoted market price on short notice is known as liquidity risk. For example, securities issued by the U.S. Treasury and larger corporations have little liquidity risk while securities issued by small and unknown companies are subject to liquidity risk. Illiquidity of a firm is the situation where the firm's maturing obligations are greater than the cash immediately available to pay.

An asset that can be sold quickly for close to its quoted price is highly liquid. An asset that cannot be sold quickly and is sold at a reduced price is not highly liquid.

(C) Inventory Management Inventories are least liquid because they take a long time to convert into cash. They can be damaged, spoiled, or stolen.

(h) Valuation Models

Three type of valuation models are discussed in this section, including inventory valuation (e.g., cost flow methods, valuation methods, and estimation methods), financial asset valuation (e.g., stocks and bonds), and business valuation (e.g., book value model, liquidation value model, and price replacement cost model).

(i) Inventory Valuation

Accounting Research Bulletin (ARB) 43, *Restatement and Revision of Accounting Research Bulletins*, defines inventory as "the sum of those items of tangible personal property which are held for sale in the ordinary course of business, in process of production for sale, or to be currently consumed in the production of goods for sale." The three types of manufacturing inventory are raw materials, WIP, and finished goods, and is the largest current asset. A committee of the American Institute of Certified Public Accountants (AICPA) said: "A major objective of accounting for inventories is the proper determination of income through the process of matching appropriate costs against revenues."

(A) Inventory Cost Flow Methods Five inventory costing methods are used based on differing inventory flow assumptions.

1. **Specific identification method**, where the cost of the specific items sold are included in the COGS, while the costs of the specific items on hand are included in the inventory. This method is used for valuing jewelry, fur coats, automobiles, and high-priced furniture.

   Advantages are accuracy; if done properly, cost flow matches the physical flow of the goods. **Disadvantages** are that it requires detailed record keeping and elaborate manual and/or computer systems.

2. **Average cost method**, where the items in inventory are priced on the basis of the average cost of all similar goods available during the period. The weighted-average method or moving-average technique is used for calculating the ending inventory and the COGS.

   The **advantage** of the average cost method is that it is simple to apply, and it is objective. The **disadvantage** is that the inventory is priced on the basis of average prices paid, which is not realistic.

3. **FIFO method**, where goods are used in the order in which they are purchased; the first goods purchased are the first used. The inventory remaining must represent the most recent purchase. Cost flow matches the physical flow of the goods, similar to the specific identification method.

   An **advantage** of the FIFO method is that the ending inventory is close to current cost and provides a reasonable approximation of replacement cost on the balance sheet when price changes have not occurred since the most recent purchases.

   A **disadvantage** of FIFO is that current costs are not matched against current revenues on the income statement. The oldest costs are charged against the more current revenue, which can lead to distortions in gross profit and net income. This creates transitory or inventory profits ("paper profits").

4. **LIFO method**, where the cost of the last goods purchased are matched against revenue. The ending inventory would be priced at the oldest unit cost. LIFO is the most commonly used method.

   The LIFO method matches the cost of the last goods purchased against revenue, and the ending inventory is costed at the oldest units remaining in the inventory. In other words, in LIFO, the inventory with current costs becomes part of the COGS for the current period, and this COGS is matched against revenues and sales for that current period. Ending inventory contains the oldest inventory with the oldest costs.

   LIFO **advantages** are listed next.

   - During periods of inflation, current costs are matched against current revenues, and inventory profits are thereby reduced. Inventory profits occur when the inventory costs matched against sales are less than the inventory replacement cost. The COGS is understated, and profit is considered overstated.
   - Lower tax payments. The tax law requires that if a firm uses LIFO for tax purposes, it must also use LIFO for FA and reporting purposes.
   - Improved cash flow due to lower tax payments, which could be invested for a return unavailable to those using FIFO.

   LIFO **disadvantages** are listed next.

   - Lower profits reported under inflationary times. The company's stock could fall.
   - Inventory is understated on the balance sheet because the oldest costs remain in ending inventory. This understatement of inventory makes the firm's working capital position appear worse than it really is.
   - LIFO does not approximate the physical flow of the items.
   - LIFO falls short of measuring current cost (replacement cost) income, though not as far as FIFO.

- Manipulation of income at the end of the year could occur by simply altering a firm's pattern of purchases.

5. **Next-in, first-out (NIFO) method**, which is not currently acceptable for purposes of inventory valuation. NIFO uses replacement cost. When measuring current cost income, the COGS should consist not of the most recently incurred costs but rather of the cost that will be incurred to replace the goods that have been sold.

KEY CONCEPTS TO REMEMBER: Inflation, LIFO, FIFO, and Taxes

- During general and prolonged inflation, income tends to be overstated because of holding gains.
- The LIFO method results in a significantly understated value of inventory when prices move up steadily. LIFO helps to exclude inventory profits from the determination of net income, resulting in lower income.
- During a period of rising prices, taxable income and income taxes are reduced through the use of LIFO.
- Under LIFO, the most recent costs of goods acquired are assigned to COGS, thus resulting in a more realistic matching of costs and revenues.
- Under the FIFO method, the inventory is valued at the most recently incurred costs; thus, the cost assigned to inventory tends to be relatively close to the current replacement cost. Earliest costs are assigned to the COGS, thus resulting in the reporting of holding gains in net income.
- During a period of rising prices, taxable income and income taxes are increased through the use of FIFO.
- The FIFO method results in a significantly overstated value of inventory when prices move up steadily.
- During inflationary periods, LIFO is usually considered preferable to FIFO. However, with LIFO, a major problem exists in evaluating inventory on the balance sheet when reviewing a company's financial statements.

(B) Inventory Valuation Methods Generally, **historical cost** is used to value inventories and COGS. In certain circumstances, though, departure from cost is justified. Some other methods of costing inventory are listed next.

- **Net realizable value.** Damaged, obsolete, or shopworn goods should never be carried at an amount greater than net realizable value. Net realizable value is equal to the estimated selling price of an item minus all costs to complete and dispose of the item.
- **Lower of cost or market.** If the value of inventory declines below its historical cost, then the inventory should be written down to reflect this loss. A departure from the historical cost principle is required when the future utility of the item is not as great as its original cost. When the purchase price of an item falls, it is assumed that its selling price has fallen or will fall. The loss of the future utility of the item should be charged against the revenues of the period in which it occurred. Market in this context generally means the replacement cost of the item.

  However, **market cost is limited by a floor and ceiling cost**. Market cannot exceed net realizable value, which is the estimated selling price minus the cost of completion and

disposal (ceiling). Market cannot be less than net realizable value minus a normal profit margin (floor). Lower of cost or market can be applied to each inventory item, each inventory class, or total inventory.

EFFECTS OF INVENTORY ERRORS

- If ending inventory is overstated, assets, gross margin, net income, and owners' equity will be overstated, and COGS will be understated.
- If ending inventory is understated, assets, gross margin, net income, and owners' equity will be understated, and COGS will be overstated.

(C) Inventory Estimation Methods An organization may estimate its inventory to compare with physical inventories to determine whether shortages exist, to determine the amount of inventory destroyed in a fire or stolen, or to obtain an inventory cost figure to use in monthly or quarterly (interim) financial statements. Two methods of estimating the cost of ending inventory are the gross margin (GM) method and the retail inventory method (see Exhibit 7.35).

- Gross margin method (establishes a relationship between gross margin and sales; prior-period gross margin rates are used to estimate the current inventory cost)
- Retail inventory method (establishes a relationship between prices and costs; cost/price ratio is used to estimate the current inventory cost)

EXHIBIT 7.35 Inventory Estimation Methods

The **gross margin method** is based on the assumption that the relationship between GM and sales has been fairly stable. GM rates from prior periods are used to calculate estimated gross margin. The estimated GM is deducted from sales to determine estimated COGS. Estimated COGS is then deducted from cost of goods available for sale to determine estimated inventory cost.

The **retail inventory method** is used by organizations that mark their inventory with selling prices. These prices are converted to cost using a cost/price (cost-to-retail) ratio. The cost/price ratio is simply what proportion cost is to each sales dollar. This cost/price ratio is applied to ending inventory stated at retail prices to estimate the cost of ending inventory.

The proper treatment of net additional markups and markdowns in the cost-to-retail ratio calculation is to include the net additional markups in the ratio and to exclude net markdowns. This approach approximates the lower-of-average-cost-or-market valuation.

Example Calculation of Inventory Lost Due to Fire

A division of a company experienced a fire in 20X2, which destroyed all but $6,000 of inventory (at cost). Data available are next.

	20X1	20X2 (to date of fire)
Sales	$100,000	$40,000
Purchases	70,000	35,000
Cost of goods sold		60,000
Ending inventory		10,000

Question: What is the approximate inventory lost (destroyed) to the fire in 20X2?

Answer: Inventory lost to the fire in 20X2 is $15,000, as shown next.

20X2 sales	$40,000
20X2 cost of goods sold using 20X1 ratio ($60,000/$100,000) × $40,000 =	$24,000 Cost of goods sold in 20X2
	$10,000 Beginning inventory 20X2
	$35,000 Purchases in 20X2
	$45,000 Goods available for sale in 20X2
	$24,000 Cost of goods sold in 20X2
	$21,000 Ending inventory in 20X2
	$6,000 Undestroyed inventory in 20X2
	$15,000 Destroyed inventory in 20X2

(ii) Financial Asset Valuation

Policy decisions that are most likely to affect the value of the firm include: investment in a project with large net present value (NPV), sale of a risky operating division that will now increase the credit rating of the entire company, and use of more highly leveraged capital structure that results in a lower cost of capital.

Establishing or predicting the value of a firm is an important task of the financial manager since maximizing the value of the firm is a major goal. Here the focus is on maximizing shareholders' wealth. Similar to capital budgeting decisions, the financial manager can use discounted cash flow (DCF) techniques to establish the worth of any assets (e.g., stocks, bonds, real estate, equipment) whose value is derived from future cash flows. *The key concept of DCF is that it takes time value of money into account. The value of a firm is a combination of bond valuation, common stock valuation, and preferred stock valuation* (see Exhibit 7.36).

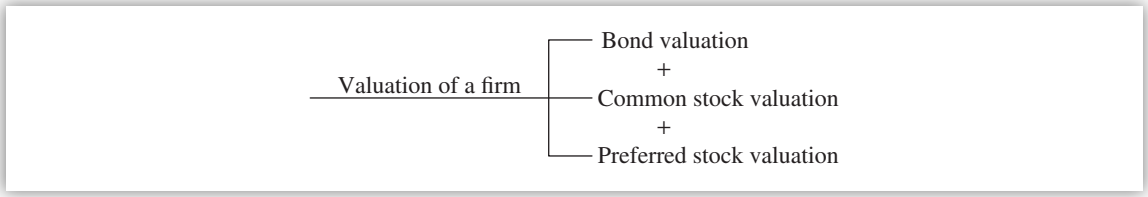


EXHIBIT 7.36 Valuation of a Firm

(A) Bond Valuation A bond valuation model shows the mathematical relationships between a bond's market price and the set of variables that determine the price. For example, bond prices and interest rates are inversely related. Corporate bonds are traded in the over-the-counter market.

DEFINITIONS OF KEY TERMS: BONDS

Call provision. A provision that allows the issuer to pay off (redeem) the bond prior to its maturity date. This provision enables issuers to substitute low-interest-rate bonds for high-interest-rate bonds. When interest rates decline, issuers can sell a new issue of low-interest-rate bonds and use the proceeds to retire the old high-interest-rate bond.

Coupon interest payment. The specified number of dollars of interest paid each period on a bond.

Coupon interest rate. The coupon interest payment divided by the par value. It is the stated amount rate of interest on a bond and remains fixed.

Maturity date. A specified date on which the par value of the bond must be repaid.

Par value. The stated face value of the bond. The par value represents the amount of money the firm borrows and promises to repay at some future date (i.e., maturity date)

Reinvestment rate risk. A bond with a shorter (e.g., one year) maturity exposes the buyer to more such risk than a bond with a longer maturity (e.g., 10 years). Reinvestment rate risk is the risk that income will decline when the funds received from maturing short-term bonds are reinvested.

Yield to call. The rate of return earned on a bond if it is called before the maturity date.

Yield to maturity. The rate of return earned on a bond if it is held to maturity.

Treasuries raise money by issuing bonds and offering common equity. A bond that has just been issued is known as a new issue. Newly issued bonds are sold close to par value. A bond that has been on the market for a while is called a seasoned issue and is classified as an outstanding bond. The prices of outstanding bonds vary from par value. A bond's market price is determined primarily by its coupon interest payments. The coupon interest payment is set at a level that will cause the market price of the bond to equal its par value.

KEY CONCEPTS TO REMEMBER: Bond Valuation

- The higher the coupon interest payment, the higher the market price of the bond.
- The lower the coupon interest payment, the lower the market price of the bond.
- At constant coupon interest payment and changing economic conditions, the market price of the bond is more or less equal to its par value.
- A bond's interest rate depends on its riskiness, liquidity, yield to maturity, and supply and demand conditions of money in the capital markets.

A bond represents an annuity (i.e., interest payments) plus a lump sum (i.e., repayment of the par value), and its value is found as the PV of this payment stream. The equation to find a bond's value is

$$\text{Value of bond} = I\,(\text{Present value of annuity}) + M\,(\text{Present value of lump sum})$$

where I = Dollars of interest paid each year (i.e., Coupon interest rate × Par value = Coupon interest payment)

M = Par (maturity) value

Both the PV of the annuity and the lump-sum amount are discounted at an appropriate rate of interest (Kd) on the bond for a number of years (n) until the bond matures. The value of n declines each year after the bond is issued.

PREMIUM VERSUS DISCOUNT OF A BOND

- When interest rates fall after bonds are issued, the value of the firm's bonds would increase, and the bonds would sell at a premium, or above its par value.

  Bond premium = Bond price + Par value

- When interest rates rise after bonds are issued, the value of the firm's bonds would decline, and the bonds would sell at a discount, or below their par value.

  Bond discount = Bond price – Par value

  The discount or premium on a bond may be calculated as follows:

  Discount or premium = (Interest payment on the old bond – Interest payment on the new bond) × PV of annuity

  The PV is calculated for *n* years to maturity on the old bond and at current rate of interest (*Kd*) on a new bond. Total rate of return or yield on a bond is equal to Interest (current yield) + Current gains yield.

A graph can be drawn to show the values of a bond in relation to interest rate changes. Note that regardless of what the future interest rates are, the bond's market value will always approach its par value as it nears the maturity date, except in bankruptcy. If the firm went bankrupt, the value of the bond might drop to zero.

KEY CONCEPTS TO REMEMBER: Interrelationships between the Coupon Interest Rate, Par Value, and Going Rate of Interest

- Whenever the going rate of interest is equal to the coupon interest rate, a bond will sell at its par value.
- Whenever the going rate of interest is greater than the coupon rate, a bond will sell below its par value. This bond is called a discount bond.
- Whenever the going rate of interest is less than the coupon rate, a bond will sell above its par value. This bond is called a premium bond.
- The longer the maturity of the bond, the greater its price changes in response to a given change in interest rates.
- An increase in interest rates will cause the price of an outstanding bond to fall.
- A decrease in interest rates will cause the price of an outstanding bond to rise.
- Those who invest in bonds are exposed to interest rate risk (i.e., a risk due to changing interest rates).
- The bond with a longer maturity is exposed to more risk from a rise in interest rates.

(B) Common Stock Valuation Investors buy common stock for two main reasons: to receive dividends and to enjoy capital gain. Dividends are paid to stockholders at management's discretion since there is no legal obligation to pay dividends. Usually stockholders expect to receive dividends, even though, in reality, they may not. If the stock is sold at a price above its purchase price, the

investor will receive a capital gain. Similarly, if the stock is sold at a price below its purchase price, the investor will suffer capital losses.

The value of a common stock is calculated at the PV of the expected future cash flow stream (i.e., expected dividends, original investment, and capital gain or loss). Different aspects of these cash flow streams involve the determination of the amount of cash flow and the riskiness of the amounts, and knowing what alternative actions affect stock prices.

Next, the stock values are determined using four different scenarios.

Scenario 1: Expected dividends as the basis for stock values

$$\text{value of stock } (Po) = \sum \frac{Dt}{(1+Ks)^t}$$

where Po = Actual market price of the stock today
Dt = Dividend the stockholder expects to receive at the end of year t (can vary from one year to infinity)
Ks = Minimum acceptable or required rate of return on the stock

Scenario 2: Stock values with zero growth. A stock reaches a zero-growth stage (i.e., $g = 0$) when future dividends are not expected to grow at all (i.e., $D1 = D2 = D3 \ldots Dn$). Dividends will be constant over time. The value of a zero-growth stock is defined as $Po = D/Ks$. Zero-growth stock is a perpetuity since it is expected to pay a constant amount of dividend each year.

Scenario 3: Stock values with normal growth. Most firms experience an increase in earnings and dividends while some firms may not. Dividends growth rate is expected to be equal to nominal gross national product (i.e., real GNP + Inflation). The value of a stock with normal (constant) growth is defined by Myron Gordon as $Po = D1/(Ks - g)$, which is called the Gordon model. When using the Gordon model, the investor's required rate of return on the firm's stock is used in determining the value of a stock. This value, in turn, is used to calculate the cost of equity.

KEY CONCEPTS TO REMEMBER: Common Stock Valuation

- A company's stock price decreases as a result of the increase in nominal interest rates.
- Growth in dividends occurs as a result of growth in EPS.
- Earnings growth, in turn, results from these factors:
  - Inflation. If output is stable and if both sales prices and input costs rise at the inflation rate, EPS will grow at the inflation rate.
  - The amount of earnings the firm reinvests. EPS will grow as a result of retained earnings.
  - The rate of return the firm earns on its equity.

Scenario 4: Stock values with supernormal growth. Some companies experience supernormal (nonconstant) growth, where their growth rate is much faster than that of the economy as a whole. The growth rate depends on what stage a company is in its business cycle (i.e., introduction, mature).

STOCK PRICES VERSUS GROWTH RATES

- The stock price of a zero-growth firm is expected to be constant.
- The stock price of a declining firm is expected to be falling.
- The stock price of a constant-growth firm is expected to grow at a constant rate.
- The stock price of a supernormal-growth firm is expected to be higher in the beginning and then to decline as the growth period ends.

(C) Preferred Stock Valuation As mentioned earlier, preferred stock is a hybrid stock—it has elements of both bonds and common stock. Most preferred stocks entitle their owners to regular fixed dividend payments. The value of the preferred stock can be found as follows:

$$Vps = \frac{Dps}{Kps}$$

where Vps = Value of the preferred stock
Dps = Preferred dividend
Kps = Required rate of return on preferred stock

(iii) Business Valuation

Business valuation means valuing the worth of a business entity, whether in whole or in part. The value of a business is derived from its ability to generate cash flows consistently period after period over the long term. Business valuation can be performed at various milestones, such as:

- New product introduction.
- Mergers, acquisitions, divestitures, recapitalization, and stock repurchases.
- Capital expenditures and improvements.
- Joint venture agreements.
- Ongoing review of performance of business unit operations.

There are 12 models to help management make sound decisions during valuation of a business opportunity. These models, in the order of importance and usefulness, are listed next.

1. Book value model
2. Accounting profit model
3. Liquidation value model
4. Replacement cost model
5. Discounted abnormal earnings model
6. Price multiples model
7. Financial analysis model
8. Economic-value-added model
9. Market-value-added model
10. Economic profit model

11. NPV model

12. DCF model

Each model is briefly discussed.

(A) Book Value Model The book value (net worth, net assets, or stockholders' equity) of a company's stock represents the total assets of the company less its liabilities. The book value per share has no relation to market value per share, as book values are based on historical cost of assets, not at the current value at which they could be sold. Book values are not meaningful because they are distorted by inflation factors and different accounting assumptions used in valuing assets. One use of book value is to provide a floor value, with the true value of the company being some amount higher. Sales prices of companies are usually expressed as multiples of book values within each industry.

(B) Accounting Profit Model Accounting profit is total revenue minus total accounting cost, which is used in the calculation of the EPS ratio. The total accounting cost is the explicit costs of production or service inputs, where these costs represent the actual monies paid to acquire inputs. The price of a product or service is often determined with accounting costs, not economic costs. The resources (e.g., labor, money, materials, energy, and machinery) used to produce goods and services are known as factors of production or simply production inputs. Accounting profits and costs are objectively determined based on the application of GAAP. The accounting profit model is mainly based on the book value model. The relationship is as follows:

$$\text{Accounting profit} = \text{Total revenues} - \text{Total explicit costs}$$

(C) Liquidation Value Model The liquidation value of a firm is total assets minus all liabilities and preferred stock minus all liquidation costs incurred. Liquidation value may be a more realistic measure of a firm than book value in that a liquidation price reflects the current market value of the assets and liabilities if the firm is in a growing, profitable industry. Depending on the power of negotiations, the liquidation prices may be set at fire-sale prices. This model requires calculating the terminal cash flows, which are the after-tax nonoperating cash flows, occurring in the final year of a project.

(D) Replacement Cost Model The replacement cost model is based on the estimated cost to replace a company's assets, which include both tangible (e.g., plant, and equipment) and intangible assets (e.g., patents, copyrights). Only tangible assets are replaceable; intangible ones are not. Because of this fact, the replacement cost is lower than the market value of the company; sometimes it could be higher than the market value.

(E) Discounted Abnormal Earnings Model If a firm can earn only a normal rate of return on its book value, then investors will pay no more than the book value. Abnormal earnings are equal to total earnings minus normal earnings. The estimated value of a firm's equity is the sum of the current book values plus the discounted future abnormal earnings.

(F) Price Multiples Model The value of a firm is based on price multiples of comparable firms in the industry. This model requires calculating of the desired price multiples and then applying the multiple to the firm being valued. Examples of price multiples include P/E ratio, price-to-book ratio, price-to-sales ratio, price-to-cash-flow ratio, and market-to-book ratio.

(G) Financial Analysis Model Financial analysis includes ratio analysis and cash flow analysis. In ratio analysis, the analyst can compare ratios for a firm over several years, compare ratios for the

firm and other firms in the industry, and compare ratios to some benchmark data. While ratio analysis focuses on analyzing a firm's income statement or its balance sheet, the cash flow analysis focuses on operating, investing, and financing policies of a firm by reviewing its statement of cash flows. Cash flow analysis also provides an indication of the quality of the information in the firm's income statement and balance sheet.

(H) Economic-Value-Added Model Economic value added (EVA) is operating profit minus a charge for the opportunity cost of capital. An advantage of the EVA method is its integration of revenues and costs of short-term decisions into the long-term capital budgeting process. Disadvantages of EVA are that it focuses only on a single period and does not consider risk. The EVA model can be combined with market-value-added (MVA) model to address this disadvantage. The formula for calculating the EVA is operating profit minus (weighted-average cost of capital [WACC] multiplied by capital invested).

(I) Market-Value-Added Model The MVA model is the difference between the market value of a company's debt and equity and the amount of capital invested since its origin. The MVA measures the amount by which stock market capitalization increases in a period. Market capitalization is simply the number of shares outstanding multiplied by share price. MVA is calculated as: PV of debt plus market value of equity minus capital invested.

(J) Economic Profit Model According to the economic profit model, the value of a company equals the amount of capital invested plus a premium equal to the PV of the cash flows created each year. Economic profit measures the value created in a company in a single period, and it is calculated as: invested capital multiplied by (return on invested capital minus WACC).

Economic profit is total revenue minus total economic cost, where (1) total revenue is the total money received from selling goods or rendering services and (2) economic cost is the total cost of inputs used in the production of goods and services; it is equal to explicit costs (product/service costs) plus implicit costs (opportunity costs). Economic costs are greater than accounting costs and economic profits are less than accounting profits because accounting costs do not include opportunity (implicit) costs. Note that the traditional corporate accounting system does not record economic profits and costs because they are subjectively determined and are not derived from the GAAP.

$$\text{Economic profit} = \text{Total revenues} - \text{Total explicit costs} - \text{Total implicit costs}$$

Opportunity cost is the cost of a forgone choice when selecting some other choice (i.e., it is the amount of sacrifice to get something). It is a trade-off between two choices and is an example of implicit cost that does not require money payments to acquire inputs. Opportunity costs should be considered in decision making and capital investments. However, opportunity costs are considered in economic costs but not in accounting costs because opportunity costs are not recorded by the formal accounting system. Examples of implicit costs include opportunity cost, cost of capital (interest costs), and cost of management talent.

$$\text{Opportunity costs} = \text{Total implicit costs}$$

(K) Net Present Value Model Basically, the NPV model compares the benefits of a proposed project or firm with the costs, including financing costs, and approves those projects or firms whose benefits exceed costs. The NPV model incorporates the time value of money and the riskiness of the cash flows, which are the vital elements of a valuation model. The approach is to calculate the NPV of each alternative and then select the alternative with the highest NPV. NPV is calculated as: PV of all cash inflows minus PV of all cash outflows.

(L) Discounted Cash Flow Model The total value of a firm is value of its debt plus value of its equity. The DCF model goes beyond the NPV model and uses free cash flows. The DCF model focuses on discounting cash flows from operations after investment in working capital, less capital expenditures. The model does not consider interest expenses and cash dividends.

The calculation involves the generation of detailed, multiple-year forecasts of cash flows available to all providers of capital (debt and equity). The forecasts are then discounted at the WACC to arrive at an estimated PV of the firm. The value of debt is subtracted from the total value of the firm to arrive at the value of equity. Note that the DCF model considers the time value of money but does not consider the riskiness and uncertainty of specific cash flows (both inflows and outflows) in terms of their amounts.

(I) Capital Budgeting Methods and Decisions Capital budgeting decisions deal with long-term future of a firm's course of action. It is the process of analyzing investment projects and deciding whether they should be included in the capital budget, which, in turn, outlines the planned expenditures on fixed assets, such as buildings, plant, machinery, equipment, warehouses, and offices.

CURRENT ASSETS VERSUS FIXED ASSETS

- Working capital decisions focus on increasing current assets.
- Investment decisions focus on increasing fixed assets.

A firm needs to develop capital budget plans several years in advance to synchronize the timing of funds availability with the timing of fixed asset acquisitions. Capital budgeting projects are initiated and selected by the company's management to be in line with the strategic business plan (e.g., M&A, introduction of new products). Generally, the larger the required investment, the more detailed the analysis and the higher the level of management approval required to authorize the expenditure.

SIMULATION AND CAPITAL BUDGETING

A firm is evaluating a large project; it wants to develop not only the best guess of the outcome of the project but also a list of outcomes that might occur. The firm would best achieve its objective by using simulation as applied to capital budgeting.

The process of capital budgeting is similar to securities valuation (i.e., stocks and bonds) in that the value of the firm increases when the asset's PV exceeds its cost. A link between capital budgeting and stock values exists in that the more effective the firm's capital budgeting procedures, the higher the price of its stock. From an economics point of view, an optimal capital budget is determined by the point where the marginal cost of capital is equal to the marginal rate of return on investment.

(i) Methods to Rank Investment Projects

Four methods used to rank investment projects and to decide whether they should be accepted for inclusion in the capital budget are: (1) payback method (regular and discounted), (2) NPV

method, (3) regular internal rate of return (IRR), and (4) modified internal rate of return (MIRR) (see Exhibit 7.37).

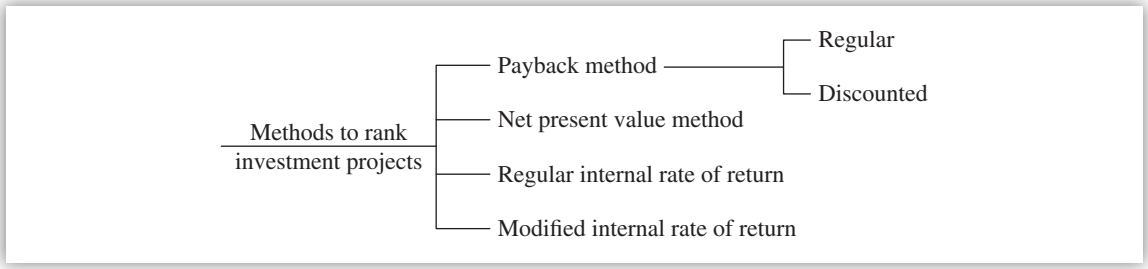


EXHIBIT 7.37 Methods to Rank Investment Projects

(A) Payback Method The payback period is investment divided by after-tax cash flows. It is the expected number of years required to recover the original investment in a capital budgeting project. The procedure calls for accumulating the project's net cash flows until the cumulative total becomes positive. The shorter the payback period, the greater the acceptance of the project and the greater the project's liquidity. Risk can be minimized by selecting the investment alternative with the shortest payback period. Initial investment money can be recouped quickly.

A variation of the regular payback method is the discounted payback period, where the expected cash flows are discounted by the project's cost of capital or the required rate of return for the project. The next list compares regular payback and discounted payback.

- A regular payback period is the number of years required to recover the investment from the project's net cash flows. It does not take into account the cost of capital. The cost of debt and equity used to finance the project is not reflected in the cash flows.
- A discounted payback period is the number of years required to recover the investment from discounted cash flows. It does take into account the cost of capital. It shows the breakeven years after covering debt and equity costs.
- Both methods are deficient in that they do not consider the time value of money.
- Both methods ignore cash flows after the payback period.

It is possible for the regular payback and the discounted payback methods to produce conflicting ranking of projects. The payback method is often used as a rough measure of both the liquidity and the riskiness of a project since longer-term cash flows are riskier than near-term cash flows. This method is used as a screening device to weed out projects with high and marginal payback periods. A low payback period is preferred. The payback method can be used to reduce the uncertainty surrounding a capital budgeting decision and is often used in conjunction with NPV and IRR methods.

(B) Net Present Value Method A simple method to accommodate the uncertainty inherent in estimating future cash flows is to adjust the minimum desired rate of return. DCF techniques, which consider the time value of money, were developed to compensate for the weakness of the payback method. Two examples of DCF techniques are the NPV method and the IRR method.

NPV is equal to the PV of future net cash flows, discounted at the marginal cost of capital. The approach calls for finding the PV of cash inflows and cash outflows, discounted at the project's cost of capital, and adding these discounted cash flows to give the project's NPV. The rationale for the NPV method is that the value of a firm is the sum of the values of its parts.

$$\text{NPV} = (\text{After-tax cash flows}) \times (\text{Present value of annuity}) - (\text{Initial investment})$$

The NPV index or profitability index is the PV of after-tax cash flows divided by initial investment. Accounting rate of return is annual after-tax net income divided by initial or average investment. When the profitability index or cost/benefit ratio is 1, the NPV is zero.

Decision Rules

- If the NPV is positive, the project should be accepted since the wealth of the current stockholders would be increased.

PRESENT VALUES AND FUTURE VALUES

The relationship between the PV of a future sum and the future value of a present sum can be expressed in terms of their respective interest rate factors. The interest factor for the future value of a present sum is equal to the reciprocal of the interest factor for the PV of a future sum.

- If the NPV is negative, the project should be rejected since the wealth of the current stockholders would be reduced.
- If the NPV is zero, the project should be accepted even though the wealth of the current stockholders is unchanged. (The firm's investment base increases but the value of its stock remains constant.)
- If two projects are mutually exclusive, the one with the higher positive NPV should be chosen.
- If two projects are independent, there is no conflict in selection. Capital rationing is the only limiting factor.
- If money is available, invest in all projects in which the NPV is greater than zero.
- If a project's return exceeds the company's cost of capital, select the combination of projects that will fully utilize the budget and maximize the sum of the NPVs.

(C) Regular Internal Rate of Return In the regular IRR method, the discount rate that equates the PV of future cash inflows to the investment's cost is found. In other words, the IRR method is defined as the discount rate at which a project's NPV equals zero. Similarities and differences between the NPV and IRR methods are listed next.

Similarities

- Both NPV and IRR methods consider the time value of money.
- Both methods use the same basic mathematical equation for solving the project's problems.

Differences

- In the NPV method, the discount rate is specified, and the NPV is found.
- In the IRR method, the NPV is specified to equal zero, and the value of IRR that forces this equality is determined.
- The NPV method assumes reinvestment of project cash flows at the cost of capital.
- The IRR method assumes reinvestment of project cash flows at the IRR.

When a project's IRR is greater than its marginal cost of capital, the value of the firm's stock increases since a surplus remains after paying for the capital. Similarly, when a project's IRR is less than its marginal cost of capital, the value of the firm's stock decreases since the project reduces the profits of the existing stockholders.

EVALUATING CAPITAL PROJECTS

The payback method, NPV method, and IRR method all show an investment "breakeven" point for the project in an accounting sense, which would be useful in evaluating capital projects. The IRR method, NPV method, and NPV index consider risk only indirectly through the selection of a discount rate used in the PV computations.

Two kinds of projects exist: normal and nonnormal. A normal project is one that has one or more cash outflows followed by a series of cash inflows. When evaluated by the IRR method, the project does not present any difficulties. However, when a nonnormal project (i.e., a project that calls for a large cash outflow either sometime during or at the end of its life) is evaluated by the IRR method, unique difficulties can arise.

Which Method Is Best: Payback, NPV, or IRR? Any capital budgeting method should meet three criteria in order to produce consistent and correct investment decisions:

1. **The method must consider all cash flows throughout the entire life of a project.** The payback method does not meet this property. The NPV and IRR methods do.
2. **The method must consider the time value of money.** A dollar received today is more valuable than a dollar received tomorrow. The payback method does not meet this property. The IRR and NPV methods do.
3. **The method must choose the project that maximizes the firm's stock price among a set of mutually exclusive projects.** The payback method and the IRR methods do not meet this property. The NPV method meet this property all the time.

The NPV method is better for evaluating mutually exclusive projects. However, when two projects are independent, both the NPV and the IRR criteria always lead to the same accept or reject decision.

The critical issue in resolving the NPV/IRR conflicts between mutually exclusive projects is the different reinvestment rate assumptions made. The reinvestment rate is the opportunity cost rate at which a firm can invest differential early year's cash flows generated from NPV or IRR methods.

The next list presents assumptions in NPV and IRR methods.

- **NPV assumptions.** The cash flows generated by a project can be reinvested at the cost of capital. The NPV method discounts cash flows at the cost of capital.
- **IRR assumptions.** The cash flows generated by a project can be reinvested at the IRR. The IRR method discounts cash flows at the project's IRR.

It has been demonstrated that the best assumption is that cash flows of projects are reinvested at the cost of capital. Therefore, the NPV method is better.

(D) Modified Internal Rate of Return Academics prefer the NPV method while business executives favor the IRR method. The reason business executives prefer the IRR method is that they find IRR "more natural" to analyze investments in terms of percentage rates of return rather than dollars of NPV.

The regular IRR method can be modified to make it a better indicator of relative profitability and hence better for use in capital budgeting. The new measure is called the modified IRR, and it is the discount rate at which the PV of a project's cost is equal to the PV of its terminal value. The terminal value is the sum of the future values of the cash inflows, compounded at the firm's cost of capital. In other words, the MIRR is the discount rate that forces the PV of the costs to equal the PV of the terminal value.

The MIRR method is better than the regular IRR method because MIRR assumes that cash flows from all projects are reinvested at the firm's cost of capital, whereas the regular IRR method assumes that the cash flows from each project are reinvested at the project's own IRR. Therefore, the MIRR method is better indicator of a project's true profitability.

MODIFIED INTERNAL RATE OF RETURN VERSUS NET PRESENT VALUE

- If two projects are of equal size, NPV and MIRR will always lead to the same project selection decision. No conflict is present.
- If the projects differ in size, conflicts can occur similar to NPV and regular IRR. NPV is better because it provides a better indicator of how much each project will cause the value of the firm to increase.
- The MIRR method is superior to the regular IRR method as an indicator of a project's "true" rate of return.

(vii) Postaudit of Capital Projects

A postaudit is a comparison of the actual and expected results (both costs and savings) for a given capital project and explanation of variances, if any. A postaudit is a good learning exercise and is practiced by most successful organizations. The lessons learned from the postaudit can be used to fine-tune forecasts of costs and benefits and to improve business operations.

The postaudit is a complicated process to review since factors occur that are beyond the control of most managers in the firm, such as demand uncertainty and unexpected deviations from plans. Actual savings may not materialize as expected due to unexpected costs. Despite these problems, conducting a postaudit of capital projects is a good approach, as long as the blame is on the process, not on the people involved.

(viii) Project Cash Flows and Risk Assessment

(A) Project Cash Flows It is important to note that capital budgeting decisions must be based on annual cash flows, not accounting income, and that only incremental cash flows are relevant to the accept or reject decision. Cash flows and accounting income can be different due to depreciation expense, which is a noncash expense. Net cash flows are obtained by adding depreciation expense to the net income after taxes.

Incremental cash flows represent the changes in the firm's total cash flows that occur as a direct result of accepting or rejecting the project. They are the net cash flow that can be traceable to an investment project.

Four special problems occur in determining incremental cash flows: (1) sunk costs, (2) opportunity costs, (3) externalities, and (4) shipping and installation costs (see Exhibit 7.38).

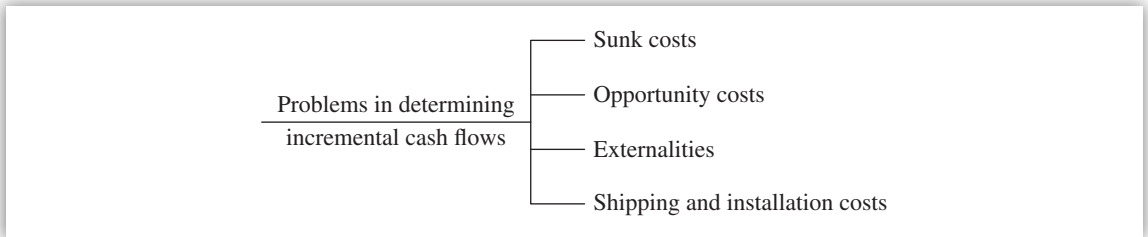


EXHIBIT 7.38 Problems in Determining Incremental Cash Flows

Sunk costs are not incremental costs, and they should not be included in the project analysis. A sunk cost is an outlay that has already been committed or has already occurred. Hence it is not affected by the "accept" or "reject" decision under consideration. Only incremental cash flows should be compared with the incremental investment.

Opportunity costs are the cash flows that can be generated from assets the firm already owns, provided they are not used for the project in question. These costs are the return on the best alternative use of an asset that is forgone due to funds invested in a particular project. Opportunity costs are not incremental costs.

Externalities are the indirect effects of a project on cash flows in other parts of the firm. Revenues produced from the effects of externalities should not be treated as incremental income.

Shipping and installation costs incurred on a new fixed asset (e.g., equipment) should be added to the invoice price of the fixed asset. The depreciation base for calculating the depreciation expense is the total invoice price including shipping and installation costs. Therefore, shipping and installation costs should not be treated as incremental cash flows; if they were, they would be double-counted.

(B) Project Risk Assessment Risk analysis is important to capital budgeting decisions. Three separate and distinct types of project risk are the project's own stand-alone risk, corporate (within-firm) risk, and market risk (beta risk) (see Exhibit 7.39).

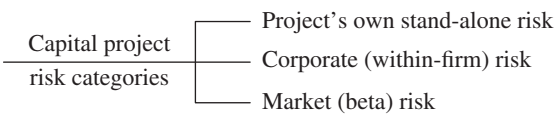


EXHIBIT 7.39 Capital Project Risk Categories

A project's **stand-alone risk** is measured by the variability of the project's expected returns. A project's **corporate risk** is measured by the project's impact on the firm's earnings variability. Corporate risk does not consider the effects of stockholders' diversification.

A project's **market (beta) risk** is measured by the project's effect on the firm's beta coefficient. Market risk cannot be eliminated by diversification. If the project has highly uncertain returns, and if those returns are highly correlated with those of the firm's other assets and with most other assets in the economy, the project will have a high degree of all types of risk. A company whose beta value has decreased due to a change in its marketing strategy would apply a lower discount rate to expected cash flows of potential projects.

Market risk is important because of its direct effect on a firm's stock prices. Both market risk and capital risk affect stock prices. Corporate risk for weak firms increases significantly compared to strong firms. This is because weak firms would have difficulty in borrowing money at reasonable interest rates, which, in turn, would decrease profits. The decrease in profits would be reflected in the price of the stock.

KEY CONCEPTS TO REMEMBER: Capital Project Risks

- It is much easier to estimate a project's stand-alone risk than its corporate risk.
- It is far easier to measure stand-alone risk than market risk.
- Stand-alone risk, corporate risk, and market risk are highly correlated.

  Economy → Firm → Project

  If the economy is good, both the firm and the projects are good, and vice versa.
- Stand-alone risk is a good proxy for hard-to-measure market risk.

Risk to a company is affected by both project variability and how project returns correlate with those of the company's prevailing business. Overall company risk will be lowest when a project's returns exhibit low variability and negative correlation.

(C) Techniques for Measuring Stand-alone Risk Here we are interested in determining the uncertainty inherent in the project's cash flows. Three techniques are available for assessing a project's stand-alone risk: sensitivity analysis, scenario analysis, and Monte Carlo simulation (see Exhibit 7.40).

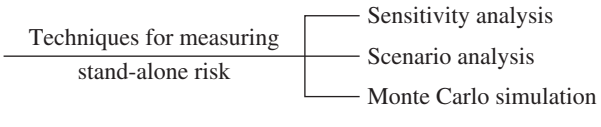


EXHIBIT 7.40 Techniques for Measuring Stand-Alone Risk

Sensitivity analysis can provide useful insights into the riskiness of a project. It is a technique that indicates exactly how much the NPV will change in response to a given change in an input variable, other things held constant. For example, if each input variable can be changed by several percentage points above and below the expected value, then a new NPV can be calculated for each of those values. Finally, the set of NPVs can be plotted against the variable that was changed. The slope of the lines in the graphs show how sensitive NPV is to changes in each of the inputs; the steeper the slope, the more sensitive the NPV is to a change in the variable.

Scenario analysis is a risk analysis technique that considers both the sensitivity of NPV to changes in key variables and the range of likely variable values. NPV is calculated under bad conditions (i.e., low sales, high variable cost per unit) and good conditions (i.e., high sales and low variable cost per unit) and compared to the expected (i.e., base case) NPV. Highlights of these relationships are shown next.

Bad condition → Worst-case scenario → (All input variables are set at their worst forecasted values)
Good condition → Best-case scenario → (All input variables are set at their best forecasted values)
Base case condition → Most likely scenario → (All input variables are set at their most likely values)

The results of the scenario analysis are used to determine the expected NPV, the standard deviation of NPV, and the coefficient of variation. Even though scenario analysis provides useful information about a project's stand-alone risk, it is limited in that it only considers a few discrete NPV outcomes for a project. In reality, there are an infinite number of outcomes.

Monte Carlo simulation ties together sensitivities and input variable probability distributions. Probability distributions of each uncertain cash flow variable are specified. The computer chooses at random a value for each uncertain variable based on the variable's specified probability distributions. The model then determines the net cash flows for each year, which, in turn, are used to determine the project's NPV in the first run. Since this is a simulation technique, this model is repeated many times to yield a probability distribution.

The primary advantage of simulation is that it shows a range of possible outcomes along with their attached probabilities. Scenario analysis shows only a few point estimates of the NPV. Both the standard deviation of the NPV and the coefficient of variation are calculated in Monte Carlo simulations, providing additional information in assessing the riskiness of a project.

It is difficult to obtain valid estimates of probability distributions and correlations among variables. From both scenario analysis and simulation analysis, no clear-cut decision rule emerges. Both techniques ignore the effects of the project as well as investor diversification—which is the major drawback.

(x) Market or Beta Risk

As mentioned earlier, beta risk is that part of a project's risk that cannot be eliminated by diversification. It is measured by the project's beta coefficient. Two methods are available to estimate the betas of individual projects: the pure-play method and the accounting beta method.

In the **pure-play method**, the company tries to find several single-product firms in the same line of business as the project being evaluated, and it then applies these betas to determine the cost of capital for its own project. A major drawback of the pure-play method is that the approach can be applied only for major assets, such as whole divisions, not individual projects. Therefore, it is difficult to find comparable business firms of the size in question.

CAPITAL ASSET PRICING MODEL TO MEASURE RISK

The capital asset pricing model (CAPM) can be used to measure market (beta) risk. A major drawback of CAPM is that it ignores bankruptcy costs. The probability of bankruptcy depends on a firm's corporate risk, not on its market risk. Therefore, management should give careful consideration to corporate risk instead of concentrating entirely on market risk.

The **accounting beta method** fills the gap of the pure-play method in finding single-product, publicly traded firms by applying against a large sample of firms. The project's beta is determined by regressing the returns of a particular company's stock against returns on a stock market index. Betas determined by using accounting data rather than stock market data are called accounting betas. In practice, accounting betas are normally calculated for divisions or other large units, not for single assets, and divisional betas are then imputed to the asset.

(xi) Project Risks and Capital Budgeting

Capital budgeting can affect a firm's market risk, its corporate risk, or both. It is difficult to develop a good measure of project risk due to difficulty in quantifying either risk.

Two methods for incorporating project risk into the capital budgeting decision process include the certainty equivalent approach and the risk-adjusted discount rate approach.

Under the **certainty equivalent approach**, the expected cash flows are adjusted to reflect project risk. All unknown cash flows will have low certainty equivalent values. This approach is difficult to implement in practice despite its theoretical appeal.

Under the **risk-adjusted discount rate approach**, differential project risk is dealt with by changing the discount rate. Risk adjustments are subjective and take these decision paths:

- Average-risk projects are discounted at the firm's average cost of capital.
- Above-average-risk projects are discounted at a higher cost of capital.
- Below-average-risk projects are discounted at a rate below the firm's average.

(xii) Capital Rationing

Although there are many acceptable capital budget projects, the amount of funds available to a firm is limited. A firm will approve an independent project if its NPV is positive. When faced with mutually exclusive projects, a firm selects the project with the highest NPV. Management cannot or would not want to raise whatever funds are required to finance all of the acceptable projects. When capital budget must be limited, this situation is called capital rationing.

Capital rationing is a constraint placed on the total size of the firm's capital investment. A drawback of capital rationing is that it is not maximizing a firm's stock value since it deliberately forgoes profitable projects. Because of this negative effect, only a few firms ration their capital.

(xiii) Key Principles and Practices in Capital Budgeting

Five key principles and practices to be employed during capital budgeting decision-making process are listed next.

Principle 1. Integrate organizational goals into the capital decision-making process.

- Practice 1a. Conduct comprehensive assessment of needs to meet results-oriented goals and objectives.
- Practice 1b. Identify current capabilities including the use of an inventory of assets and their condition, and determine if there is a gap between current and needed capabilities.

- ☐ Practice 1c. Decide how best to meet the gap by identifying and evaluating alternative approaches.

Principle 2. Evaluate and select capital assets using an investment approach.

- ☐ Practice 2a. Establish review and approval framework.
- ☐ Practice 2b. Rank and select projects based on established criteria.
- ☐ Practice 2c. Decide a long-term capital plan that defines capital asset decisions.

Principle 3. Balance budgetary control and managerial flexibility when funding capital projects.

- ☐ Practice 3a. Budget for projects in useful segments.
- ☐ Practice 3b. Consider innovative approaches to full up-front funding.

Principle 4. Use project management techniques to optimize project success.

- ☐ Practice 4a. Monitor project performance and establish incentives for accountability.
- ☐ Practice 4b. Use cross-functional teams to plan for and manage projects.

Principle 5. Evaluate results and incorporate lessons learned into the decision-making process.

- ☐ Practice 5a. Evaluate results to determine if organization-wide goals have been met.
- ☐ Practice 5b. Evaluate the decision-making process; reappraise and update to ensure those organization-wide goals are met.

(xiv) International Capital Budgeting

The techniques presented in this section for domestic capital budgeting are equally applicable to the international capital budgeting process. However, three types of risks exist in the international area: cash flow risk (i.e., cash flow estimation is much more difficult); (2) exchange rate risk (i.e., exchange rate fluctuations add to the riskiness of the foreign investment); and sovereignty risk (i.e., the possibility of deliberate foreign government acts that reduce or eliminate cash flows).

In terms of cash flows, the relevant cash flows are the dollar cash flows that the subsidiary can turn over to the parent. Since the foreign currency cash flows turned over to the parent must be converted to U.S. dollar values by translating them at expected future exchange rates, an exchange rate premium should be added to the domestic cost of capital. This is done to reflect the exchange rate risk inherent in the investment. The exchange rate risk can be minimized by hedging, which adds to the cost of the project.

Sovereignty risk includes the possibility of expropriation or nationalization without adequate compensation and also the possibility of unanticipated restrictions of cash flows to the parent company, such as tighter controls on repatriation of dividends or higher taxes. Generally, sovereignty risk premiums are not added to the cost of capital to adjust for sovereignty risk. Companies can take three major steps to reduce the potential loss from expropriation: (1) finance the subsidiary with local sources of capital, (2) structure operations so that the subsidiary has value only as a part of the integrated corporate system, and (3) obtain insurance against economic losses from expropriations. When insurance is obtained, its cost should be added to the project's cost.

(j) Cost of Capital Evaluations

The rate of return on a security to an investor is the same as the cost of capital to a firm, which is a required return on its investments. Any increase in total assets of a firm's balance sheet must be financed by an increase in one or more of capital components (i.e., debt, preferred stock, retained earnings, common stock). Like any other resources, capital has a cost. The cost of capital must reflect the average cost of the various sources of long-term funds used (i.e., one or more of the capital components used; see Exhibit 7.41). Next we briefly review each component of capital.

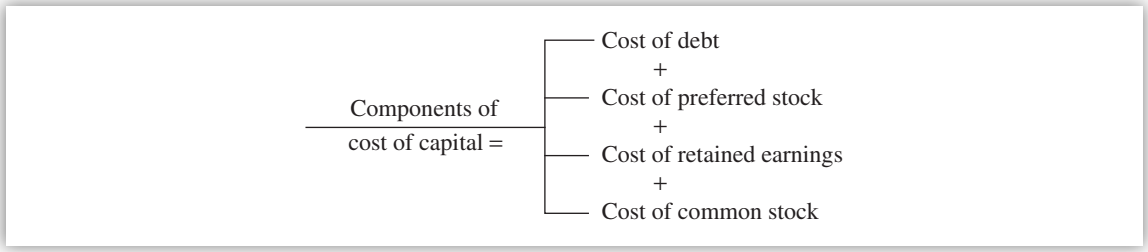


EXHIBIT 7.41 Components of Cost of Capital

(i) Cost of Debt

The cost of debt is calculated as Kd (1– T), where Kd is the interest rate on debt and T is the firm's marginal tax rate. The government pays part of the cost of debt (equal to tax rate) because interest is deductible for tax purposes. The value of the firm's stock depends on after-tax cash flows. Here we are interested in acquiring a new debt (marginal cost of debt) to finance a new asset, and past financing is a sunk cost and is irrelevant for cost of capital calculation purposes.

The key point is to compare the rate of return with after-tax flows. After-tax cost of debt is less than before-tax cost due to tax savings resulting from an interest expense deduction that reduces the net cost of debt.

(ii) Cost of Preferred Stock

The cost of preferred stock (Kp) is the preferred dividend (Dp) divided by the net issuing price (Pn) or the price the firm receives after deducting flotation costs. This is $Kp = Dp/Pn$. Since preferred dividends are not tax deductible, there are no tax savings, unlike interest expense on debt.

(iii) Cost of Retained Earnings

If management decides to retain earnings, an opportunity cost is involved (i.e., stockholders could have received the earnings as dividends and invested this money somewhere else). Because of this opportunity cost, the firm should earn on its retained earnings at least as much as the stockholders themselves could earn in alternative investments of comparable risk, such as the cost of common stock equity.

WHO REQUIRES WHAT?

- The costs of debt are based on the returns investors require on debt.
- The costs of preferred stock are based on the returns investors require on preferred stock.
- The costs of retained earnings are based on the returns stockholders require on equity capital (e.g., common stock).

(iv) Cost of Common Stock

The cost of common stock (*Ke*) is higher than the cost of retained earnings (*ks*) due to flotation costs involved in selling new common stock. The equation is

$$Ke = \frac{D1}{Po\,(1-F)} + g$$

where $D1$ = Dividends
Po = Stock price
F = Percentage flotation cost incurred in selling the new stock
$Po\,(1-F)$ = Net price per share received by the firm
g = Stock's expected growth rate

When a stock is in equilibrium, its required rate of return (*Ks*) should be equal to its expected rate of return (*Kes*).

$$Ks = Krf = Rp \text{ or } Kes = (D1/Po) + g$$

where Krf = Risk-free rate
Rp = Risk premium
$D1/Po$ = Stock's dividend yield
g = Stock's expected growth rate

Three methods are commonly used to calculate the cost of common stock: the CAPM approach, the bond-yield-plus-risk-premium approach, and the discounted cash flow (DCF) approach (see Exhibit 7.42). The DCF approach does not consider risk explicitly; the other two approaches do consider risk explicitly.

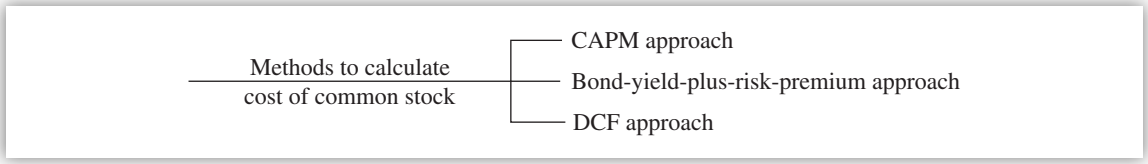


EXHIBIT 7.42 Methods to Calculate the Cost of Common Stock

(A) Capital Asset Pricing Model Approach The CAPM model is used to determine the required rate of return on an asset, which is based on the idea that any asset's return should be equal to the risk-free rate of return plus a risk premium rate that reflects the asset's non diversifiable risk. Note that the nondiversifiable risk cannot be eliminated through diversification because it is a part of systematic risk.

The CAPM model equation is:

$$Ks = Krf + (Km - Krf)\,bi$$

where Krf = Risk-free rate (e.g., U.S. Treasury bond or bill rate)
$(Km - Krf)$ = Risk premium
Km = Expected rate of return on the market or on "average" stock
bi = Stock's beta coefficient (an index of the stock's risk)

Drawbacks of the CAPM approach include:

- A stockholder may be concerned with total risk rather than with market risk only.
- Beta coefficient may not measure the firm's true investment risk.

- This approach understates the correct value of the required rate of return on the stock, *Ks.*
- It is difficult to obtain correct estimates of the inputs to the model to make it operational.

Examples of the CAPM approach include: deciding whether to use long-term or short-term Treasury bonds for the risk-free rate, difficulty in estimating the beta coefficient that investors expect the firm to have in the future, and difficulty in estimating the market risk premium.

(B) Bond-Yield-Plus-Risk-Premium Approach This method provides a ballpark estimate of the cost of equity, not a precise number, since it uses ad hoc, subjective, and judgmental estimates.

$$Ks = \text{Bond rate} + \text{Risk premium}$$

A firm's cost on common equity is found by adding a risk premium (say, 2–4%) based on judgment to the interest rate on the firm's own long-term debt.

(C) Discounted Cash Flow Approach The DCF approach is also called the dividend-yield-plus-growth rate approach, and calculated as

$$Ks = Kes = D1/Po + \text{Expected growth } (g)$$

Investors expected to receive a dividend yield ($D1/Po$) plus a capital gain (g) for a total expected return of *Kes*. At equilibrium, this expected return would be equal to the required return (*Ks*).

$$Ks = Kes$$

EFFECTS OF COST OF COMMON STOCK

- The firm must earn more than the cost of common stock (*Ke*) due to flotation cost.
- When a firm earns more than *Ke*, the price of the stock will rise.
- When a firm earns exactly *Ke*, EPS will not fall, expected dividend can be maintained, and consequently the price per share will not decline.
- When a firm earns less than Ke, then earnings, dividends, and growth will fall below expectations, causing the price of the stock to decline.

(v) Weighted-Average and Marginal Cost of Capital Concepts

An optimal (target) capital structure is a mix of debt, preferred stock, and common stock that maximizes a firm's stock price. The goal of the finance manager should be then to raise new capital in a manner that will keep the actual capital structure on target over time. The firm's WACC is calculated based on the target proportions of capital and the cost of the capital components, all based on after-tax costs. The WACC could be used as a hurdle rate for capital investment projects and is computed as:

$$\text{WACC} = WdKd\,(1 - T) + WpKp + WsKs$$

where Wd = Weight used for debt
Wp = Weight used for preferred stock
Ws = Weight used for common stock

The weights could be based on either book values or market values. The latter is preferred over the former. If a firm's book value weights are close to its market value weight, book weights can be used.

As the firm tries to raise more money, the cost of each dollar will rise at some point. The marginal cost concept can be applied here: *The marginal cost of any item is the cost of another unit of that item, whether the item is labor or production. The marginal cost of capital (MCC) is the cost of the last dollar of new capital that the firm raises, and the MCC rises as more and more capital is raised during a given period.* The MCC schedule shows how the WACC changes as more and more new capital is raised during a given year.

KEY CONCEPTS TO REMEMBER: Breakpoint, Investment Opportunity Schedule, and Marginal Cost of Capital

- A break point will occur in the MCC whenever the cost of one or more of the capital components rises. If there are n separate breaks, there will be $n + 1$ different weighted-average costs of capital.
- The investment opportunity schedule (IOS) is a graph of the firm's investment opportunities, with the projects having the highest return plotted first.
- The intersection of the MCC schedule and the IOS schedule is called the corporate cost of capital, which is used to evaluate average-risk capital budgeting projects.

The break point is the dollar value of new capital that can be raised before an increase in the firm's WACC occurs. The break point is the total amount of lower cost of capital of a given type divided by a fraction of this type of capital in the capital structure.

(vi) Issues in Cost of Capital

There are three major issues in cost of capital: depreciation-generated funds, privately owned and small business firms, and measurement problems.

1. **Depreciation-generated funds.** Depreciation is a source of capital, and its cash flows can be either reinvested or returned to investors. The cost of depreciation-generated funds is equal to the WACC in which capital comes from retained earnings and low-cost debt.
2. **Privately owned and small business firms.** The same principles of cost of capital estimation can be applied to both privately held and publicly owned firms. Input data are difficult to obtain for privately owned firms since their stock is not publicly traded.
3. **Measurement problems.** It is difficult to estimate the cost of equity, obtain input data for the CAPM approach, estimate stock growth rate, and assign different risk-adjusted discount rates to capital budgeting projects of differing degrees of riskiness.

Capital budgeting and cost of capital estimates deal with *ex ante* (estimated) data rather than *ex post* (historical) data. Because of this, we can be wrong about the location of the IOS schedule and the MCC schedule. Consequently, a project that looked good could turn out to be a bad one. Despite these issues, the cost of capital estimates used in this section are reasonably accurate. By solving these issues, refinements can be made.

(k) Taxation Schemes

Taxes are assessed for various purposes, such as to collect revenues, encourage or discourage different kinds of investments, or redistribute income among citizens. There are different types of taxes; they differ in:

- Classes of taxable income.
- Which expenses are allowed for deduction from revenues and how they are to be calculated.
- What kind of taxes (e.g., direct or indirect) are to be collected.
- The extent to which companies report income honestly.

Exhibit 7.43 presents different types of taxes.

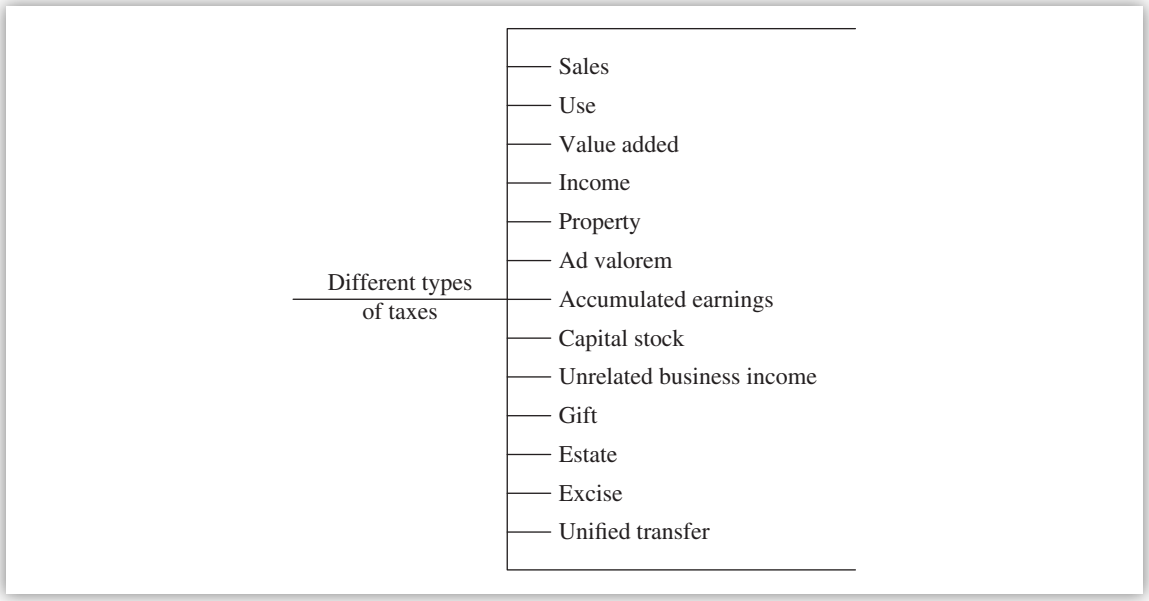


EXHIBIT 7.43 Different Types of Taxes

(i) Sales Tax

A sales tax is a state-level or local-level (e.g., county, city) tax on the retail sale of specified property. Generally, the purchaser pays the tax, but the seller collects it, as an agent for the government. Various taxing jurisdictions allow exemptions for purchases of specific items, including certain foods, services, and manufacturing equipment. If the purchaser and seller are in different states, a use tax usually applies.

THREE CONCEPTS OF AN INCOME TAX SYSTEM

A tax system should be equitable and nondistorting. Three different concepts of equity as it applies to the tax system include: (1) the ability-to-pay principle, (2) the benefit principle, and (3) equal treatment of those equally situated.

Ability-to-pay principle. Under this concept, people with higher incomes should pay more than those with lower incomes. It is based on the assumption that a more equal distribution of income would be more equitable. The real question is at what rate should different incomes be taxed. Some argue that the tax rate should be **proportional**—that is, the same percentage of each person's income.

Some argue that the tax rate should be **progressive**—that is, a higher-percentage tax on high incomes than on low incomes. All ability-to-pay advocates argue against **regressive** taxation, which takes a larger percentage of income from lower-income groups. Regressive taxes will not take a larger absolute amount of income as income rises. There is no objective way of deciding whether tax rates should be proportional or progressive or, if progressive, how steeply progressive.

Benefit principle. This concept proposes that people should be taxed only to pay for the benefits they choose to buy from the government. This concept is more revolutionary in that each individual should have the income that he or she earns by helping to produce what consumers choose to buy. A direct sale of government services to the user would prevent redistribution of income.

Equal treatment of those equally situated. This concept states that persons equally situated should be taxed equally. The term "equally situated" is not clear and may have many meanings. Are two people with the same income always equally situated? What about the differences among disabled people, or retired persons and healthy young persons with the same income?

(ii) Use Tax

A use tax is a sales tax that is collectible by the seller when the purchaser is domiciled in a different state.

(iii) Value-Added Tax

A value-added tax (VAT) is a form of sales tax. Many European countries use VATs. The firm pays a percentage of tax based on the value that its production process adds to the final product. VAT is less complex and easier to calculate than an income tax and is easier to monitor. VAT encourages honesty whereas income tax does not.

(iv) Income Tax

Income tax is a tax imposed on income earned after deducting allowable expenses from all sources of revenues. Income tax rates vary depending on the amount of income earned. Corporations are subject to an alternative minimum tax (AMT), which has a more expansive tax base than does the regular tax. The corporation is required to apply a minimum tax rate to the expanded base and pay the difference between the AMT tax liability and the regular tax.

(v) Property Tax

Property tax is an ad valorem tax, usually levied by a city or county government, on the value of real or personal property that the taxpayer owns on a specified date. Most states exclude intangible property and assets owned by exempt organizations from the tax base; some exclude inventory, pollution control, or manufacturing equipment and other items to provide relocation or retention incentives to the taxpayer.

(vi) Ad Valorem Tax

An ad valorem tax is a tax imposed on the value of property. The most common ad valorem tax is that imposed by states, counties, and cities on real estate. Ad valorem taxes can, however, be imposed on personal property as well.

(vii) Accumulated Earnings Tax

An accumulated earnings tax is a special tax imposed on corporations that accumulate (rather than distribute) their earnings beyond the reasonable needs of the business. The accumulated

earnings tax and related interest are imposed on accumulated taxable income in addition to the corporate income tax.

(viii) Capital Stock Tax

A capital stock tax, which is a state-level tax, is usually imposed on out-of-state corporations for the privilege of doing business in the state. The tax may be based on the entity's apportionable income or payroll or on its apportioned net worth as of a specified date.

(ix) Unrelated Business Income Tax

Unrelated business income tax is levied on the unrelated business taxable income of an exempt organization.

(x) Gift Tax

A gift tax is a tax imposed on the transfer of property by gift. Such tax is imposed on the donor of a gift and is based on the fair market value of the property on the date of the gift.

(xi) Estate Tax

An estate tax is a tax imposed on the right to transfer property by death. Thus, an estate tax is levied on the decedent's estate, not on the heir receiving the property.

(xii) Excise Tax

An excise tax is a tax on the manufacture, sale, or use of goods or on the carrying on of an occupation or activity, or a tax on the transfer of property. Thus, the federal estate and gift taxes are theoretically excise taxes.

(xiii) Unified Transfer Tax

Unified transfer tax is a set of tax rates applicable to transfers by gift and death made after 1976. It is a tax imposed on the transfer of property.

(I) Differences Between Tax Reporting and Financial Reporting

The net income computed for FA purposes will be different from taxable income reported on the corporation's income tax return. Therefore, reconciliation between these two types of income is essential to ensure accuracy. The starting point for the reconciliation is net income per books, which is the FA net income. Additions and subtractions are entered for items that affect net income per books and taxable income differently.[1]

Net income per books
+ Additions
– Subtractions
= Taxable income

The following items are added to the net income per books:

- Federal income tax liability (deducted in computing net income per books but not deductible in computing taxable income)
- Excess of capital losses over capital gains (deducted for FA purposes but not deductible by corporations for income tax purposes)

[1] William H. Hoffman, William A. Raabe, and James E. Smith, *Corporations, Partnerships, Estates, and Trusts* (St. Paul, MN: West's Federal Taxation, 1993).

- Income that is reported in the current year for tax purposes that is not reported in computing net income per books (e.g., prepaid income)
- Various expenses that are deducted in computing net income per books but not allowed in computing taxable income (e.g., charitable contributions in excess of the 10% ceiling applicable to corporations)

The following items are subtracted from the net income per books:

- Income reported for FA purposes but not included in taxable income (e.g., tax-exempt interest)
- Expenses deducted on the tax return but not deducted in computing net income per books (e.g., a charitable contributions carryover deducted in a prior year for FA purposes but deductible in the current year for tax purposes. The result is taxable income before net operating loss deduction and the dividends received deduction.)

(m) Mergers, Acquisitions, and Divestitures

This section discusses M&A as one topic due to their similarities; divestitures are presented as a separate topic due to their uniqueness from M&A; leveraged buyouts are discussed briefly; advantages and disadvantages of holding companies are highlighted briefly; the role of investment banker in mergers, acquisitions, and divestitures is discussed; and key terms, actions, and tactics used in M&A and divestitures are pointed out for a better understanding of the complex subject matter. Similarities and differences between acquisitions and divestitures are also presented.

(i) Mergers and Acquisitions

A merger or acquisition is defined as the combination of two or more firms to form a single large firm. An acquiring company is a firm in a merger transaction is attempting to acquire or buy another firm. A target company is a firm in a merger transaction that the acquiring company is attempting to buy or combine.

A merger can be friendly or hostile, depending on some unknown situations that can occur (e.g., changes in management's attitudes and behaviors) that are beyond each party's control. In a friendly merger, the terms and conditions of a merger are approved by the management of both companies; in a hostile merger, the target firm's management resists acquisition, leading to use takeover defenses to fight the takeover. Of course, a friendly merger is better than a hostile one.

It has been pointed out that many mergers today are designed to benefit managers of the firm more than stockholders—who are really the owners of the firm. Five motives were given to account for the high levels of U.S. merger activity and for the huge amounts of money spent using cash, stock, or both:

1. Synergy
2. Tax considerations
3. Purchase of assets below their replacement cost
4. Diversification
5. Maintaining control

(See Exhibit 7.44.)

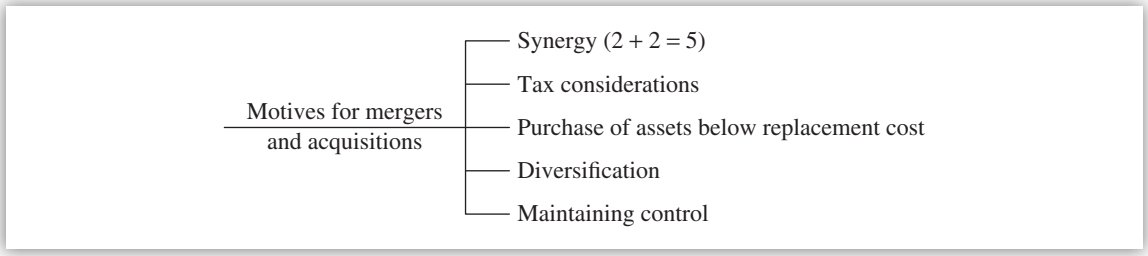


EXHIBIT 7.44 Motives for Mergers and Acquisitions

Synergy is known as the whole is greater than the sum of the parts (i.e., 2 + 2 = 5). It means outputs are more than the sum of inputs. Synergy is the basic rationale for any operating merger. The word also refers to when a company's income and stock prices are higher than before, but only after it acquired another company. Synergistic effects can arise from four sources:

1. Operating economies of scale in production or distribution
2. Financial economies, which include a higher price/earnings ratio, a lower cost of debt, or a greater debt capacity
3. Differential management efficiency (one firm's management is seen as inefficient)
4. Increased market power resulting from reduced competition

Tax considerations include using tax status to the firm's advantage and using excess cash in mergers. Using excess cash to acquire another firm has no immediate tax consequences for either the acquiring firm or its stockholders.

TAXES AND ACQUISITIONS

- A firm that is highly profitable and in the highest tax brackets could acquire a company with large accumulated tax losses, then use those losses to offset its own income. This method reduces the total tax bill and is one reason for making the acquisition.
- A firm with large losses could acquire a profitable firm and minimize the tax bill. Example: A young profitable company acquires an older company in a different industry that has experienced losses recently.

When the **replacement value of a firm's assets** is considerably higher than its market value, the firm becomes an acquisition candidate. The purchase price will be less than the replacement value of the assets.

Diversification was thought to be a stabilizing factor on a firm's earnings and thus reduce risk. There is a controversy about this practice. Stabilization of earnings is beneficial to a firm's employees, suppliers, and customers, but its value to stockholders and debt holders is not clear. This is because investors can diversify their risk on their own; a merger is not the answer.

Maintaining control is a major motivation and based on human psychology. The managers of acquired companies generally lose their jobs or their autonomy. Therefore, managers who own less than 51% of the stock in their firms look to mergers that will lessen the chances of their firm's being taken over. Defensive merger tactics are practiced by using much higher debt to acquire other firms so that the debt level will be hard for any potential acquirer to digest.

(A) Types of Mergers Economists classify mergers into five groups:

1. Horizontal
2. Vertical
3. Congeneric
4. Conglomerate
5. Beachhead

(See Exhibit 7.45.)

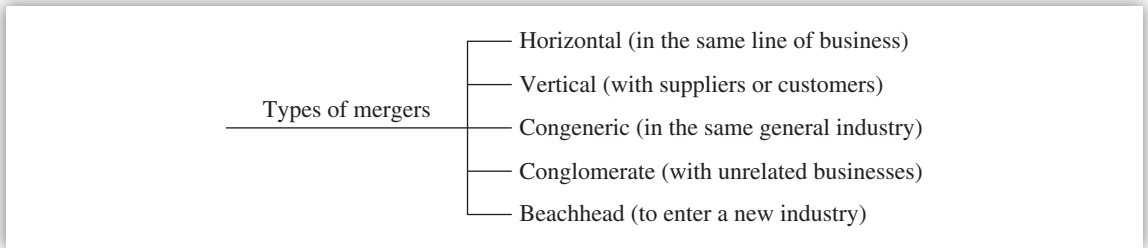


EXHIBIT 7.45 Types of Mergers

A **horizontal merger** occurs when one firm combines with another competing firm in its same line of business or market. Such a merger can occur between a producer and another producer in the same industry (e.g., an automobile manufacturing firm combines with another automobile manufacturing firm). This kind of merger provides the greatest synergistic operating benefits and could be subjected to investigations by the U.S. Department of Justice or SEC. It is most likely to be attacked as a restraint of trade because both companies are in the same line of business and in the same industry.

A **vertical merger** occurs between a firm and one of its suppliers or customers. The goal is to integrate operations from both sides. It can occur between a producer and its supplier (e.g., a steel manufacturing firm acquires one of its own suppliers or customers). The suppliers are the firm's own suppliers in the supply-chain line. Two types of vertical merger can occur: (1) A forward vertical merger occurs when a supplier acquires a customer; (2) a backward vertical merger occurs when a customer acquires a supplier.

A **congeneric merger** is a merger of firms in the same general industry but for which no customer or supplier relationship exists. Also, the lines of businesses are different. Here "congeneric" means "allied in nature or action" involving related businesses. It is neither a horizontal merger nor a vertical merger.

A **conglomerate merger** occurs when two or more unrelated enterprises combine. It is an acquisition by one company of another that is not a competitor, customer, or supplier. An example is when a retail firm acquires both a financial institution and a real estate firm.

A **beachhead merger** takes on a new risk and opportunity, entering a new industry to exploit perceived opportunities.

(B) Merger Analysis Whatever type of merger is used, the underlying concept of merger analysis is capital budgeting techniques. The objective is to determine whether the PV of the cash flows expected to result from the merger exceeds the price that must be paid for the target company. The acquiring firm performs the capital budgeting analysis.

CAPITAL BUDGETING TECHNIQUES AND MERGERS

- If the NPV is positive, the acquiring firm acquires the target firm.
- If the NPV is negative, the acquiring firm does not acquire the target firm.

The merge analysis can focus on four areas, such as a strategic merger, an operating merger, a financial merger, or a strategic alliance arrangement. In a **strategic merger**, the economies-of-scale concept is the focus, which means:

- Increasing market share for products and services.
- Eliminating duplicate functions, departments, divisions, manufacturing plants, warehouses, or offices.
- Reducing the raw material suppliers' source base.
- Decreasing the number of marketing distribution channels.
- Increasing the overall efficiency of the entire company.

Senior management expects that after a strategic merger, the performance of the postmerged firm is significantly better than that of the premerged firm. A strategic merger appears to be best type of merger due to its long-term survivability or sustainability compared to other types of mergers.

An **operating merger** is a merger in which operations of the firms involved are integrated in the hope of achieving synergistic benefits. In most cases, an operating merger is similar to a strategic merger in terms of common goals and objectives to achieve.

ANALYTICAL TECHNIQUES USED IN MERGERS, ACQUISITIONS, AND DIVESTITURES

- Strengths, weaknesses, opportunities, and threats (SWOT) analysis
- Investment analysis (capital budgeting, NPV, and internal rate of return)
- Sensitivity analysis (using what-if questions, finding out what it is, and knowing what it should be after changing the inputs to determine corresponding outputs)
- Scenario analysis (building scenarios such as A, B, C, or D with best case, most likely, and worst-case outcomes with or without the help of simulations)
- Simulation analysis (using computers, models, and statistics to determine different outcomes with different assumptions)
- Normal due diligence reviews (initial screening, analysis, and negotiations) prior to closing the M&A (If such reviews are done properly, the defendant is not liable.)
- Reverse due diligence reviews (initial screening, analysis, and negotiations) prior to closing the divestitures (If such reviews are done properly, the defendant is not liable.)
- Fit-gap analysis (how much fit is there, how much gap is there, and where is the real value)
- Consequence-based analysis (understanding competitors' unexpected and aggressive moves; government's negative reactions by the SEC and Federal Trade Commission in the United States; current customers' acceptance and retention rates; changes in technology in both IT and non-IT areas; buyers becoming competitors in divestitures; positive or negative impact on sales, costs, profits, stock prices, and business growth levels; and employee morale issues)

A **financial merger** is one in which the merged companies will be operated independently and from which no significant operating economies of scale are expected. The postmerger cash flows are simply the sum of the expected cash flows of the two companies if they continued to operate independently. A financial merger also means restructuring the acquired company to improve the cash flows and unlock its hidden value.

A **strategic alliance arrangement**, although not a merger in its true meaning, occurs when a large and highly established company with proven products, markets, and distribution channels wishes to invest its money in a small and emerging company in the areas of new R&D activities that could help the large company in its growth.

After completing the merger analysis, a value of the target firm should be assessed in order to determine an educated price. Both cash flows and a discount rate are essential in valuing the target firm, although accurate estimates of future cash flows are difficult to obtain. Cash flows can be developed using a set of pro forma income statements and balance sheets for a number of years (say, five years). These net cash flows are discounted at the firm's overall cost of capital, if both debt and equity are used to finance the merger. If only equity is used, then the firm's cost of equity should be used. The price paid to acquire the target firm is a summation of the discounted net cash flows at the appropriate cost of capital.

Example Reason for Acquisition

A company acquired an older and more established competitor in the same industry. The company being acquired had consistently earned lower (but positive) net income and has a low debt-to-equity ratio. The reason for the acquisition probably was to increase financing capacity.

(ii) Divestitures

While M&A focus on buying new businesses and new assets from outside sellers either as a whole or in parts, divestitures focus on selling a company's existing businesses or assets to outside buyers either as a whole or in parts. The reason divestitures are undertaken is that these businesses or assets have little or no value to the selling company due to their underperformance or money losses and the fact that they do not fit with the core business of the selling company.

Divestiture actions can be thought of as cleaning up or strengthening the balance sheet or cleaning the closet or garage. They also can be thought of as treating nonproducing assets the same as dead assets (assets that are not making the company money and at the same time are cluttering the balance sheet). These nonproducing assets should not be taken lightly because their hidden values could be valuable to some other companies.

At least two forms of divestitures can exist: spin-offs and other types of divestitures.

1. Spin-off is a type of divestiture n which an operating division or a business unit becomes an independent company through the issuance of shares in it, on a pro rata basis, to the parent company's shareholders. The term also refers to when a company sells one of its operating divisions to its existing shareholders, and the shareholders receive new stock representing separate ownership rights in the division.
2. Other types of divestiture can include selling the entire business or assets, whether as a whole or in parts. The total value of a firm is greater than the sum of the values of its

individual operating units if each unit were sold separately. This means some units are good (hidden value) while other units are bad.

(iii) Leveraged Buyouts

Often, a leveraged buyout (LBO) method is an alternative to a merger. An LBO is a financial transaction in which a firm's publicly owned stock is bought up in a mostly debt-financed tender offer. The result is a privately owned and highly leveraged firm. There is a controversy whether LBOs are a good or a bad idea for a company or the economy as a whole. Some argue that LBOs might destabilize the economy because of the disruptive forces involved in the deal. Others argue that LBOs can stimulate lethargic or complacent management.

The existence of potential bargains, situations in which companies were using insufficient leverage, and the development of the so-called junk bond market all facilitated the use of leverage in takeovers. LBOs can be initiated in one of two ways.

1. The firm's own managers can set up a new company whose equity comes from the managers themselves plus equity from outside sources. This new company then arranges to borrow a large amount of money by selling junk bonds through an investment-banking firm.
2. A specialized LBO firm identifies a potential target company, goes to the management, and suggests that an LBO deal be done.

Whatever method is used in an LBO, the newly formed company will have a high debt ratio, ranging from 80% to 98%, hence the term "highly leveraged."

(iv) Holding Companies

A holding company is a company that owns stock in another company and exercises control. The holding company is called the parent company, and the controlled companies are called subsidiaries or operating companies. A holding company is taxed on profits, cannot issue tax-free bonds, and is subject to normal government regulations. Consolidation accounting–type transactions are needed between the parent company and its subsidiaries.

Although holding companies have advantages and disadvantages similar to those of large corporations, they differ in the following areas. Advantages of a holding company include: (1) control with fractional ownership (anywhere between 5% and 100% of another company's stock; 10% to 25% of common stock ownership is considered as having a working control); (2) isolation of risk to a single unit; and (3) legal and accounting separation when regulations make such separation desirable.

Disadvantages of a holding company include: partial multiple taxation due to not requiring a consolidated tax return when the ownership is less than 80% of a subsidiary's voting stock and ease of enforced dissolution by the Justice Department if it finds the ownership of a holding company unacceptable. The parent company is required to pay tax on dividends from the subsidiary, thus leading to partial and multiple taxations.

(v) Role of Investment Bankers in Mergers, Acquisitions, and Divestitures

An investment banker and a lawyer are usually involved with a merger by helping to arrange mergers, advising target companies in developing and implementing defensive tactics, and helping to value target companies. An investment banker is also consulted for divestitures. For these services, a fee and commissions are paid to the investment banker.

(vi) Key Terms, Actions, and Tactics Used in Mergers, Acquisitions, and Divestitures

Business mergers can be friendly or hostile. Of particular importance is developing defensive tactics to block hostile mergers. Some commonly used tactics are listed next.

- Changing the bylaws to require a supermajority of directors instead of a simple majority to approve a merger
- Educating the target firm's stockholders that the price being offered is too low
- Raising antitrust issues in the hope that the Justice Department will intervene
- Persuading a white knight more acceptable to the target firm's management that it should compete with the potential acquirer
- Taking a "poison pill," which includes:
  - Management committing suicide to avoid a takeover
  - Borrowing on terms that require immediate repayment of all loans if the firm is acquired
  - Selling off the assets at bargain prices to make the firm less attractive to the potential acquirer
  - Granting lucrative golden parachutes to the firm's executives to drain off some cash
  - Taking on a huge debt
  - Leaving behind assets of questionable value

Corporate management often uses the following terms, actions, and tactics during the merger, acquisition, and divestiture processes either to delay the process or to deny the offer, especially if it is a hostile one. In M&A, one firm is targeting to buy another firm either in part or whole with an offer to start the process. Specific examples of these terms, actions, and tactics follow.

- A **friendly merger** is a merger whose terms are amicable and approved by management of both the acquiring and the target firms. There is a higher chance of completing the friendly merger transaction and a small chance of becoming a hostile merger.
- A **tender offer** occurs when one firm buys the stock of another firm by going directly to the stockholders, frequently over the opposition of the target firm's management. The intent is to bypass the target firm's management. This is an example of a defensive takeover attempt.
- A **golden parachute** is a legal employment contract in which a corporation agrees to make payment to key officers (e.g., directors, executives, and managers) if a hostile takeover or a major change in the control of the corporation takes place. This is an added financial incentive for key officers to aggressively focus on M&A of other companies and stop worrying about their fear of job loss and losses of: bonuses, stock options, profit sharing, job status and prestige, and perks. A major downside of the golden parachute is that key officers get paid huge amounts of money even though their company's financial and operational performance is bad or not as expected. This occurs because the golden parachute is based on a legal employment contract. Here the golden parachute is used in a hostile merger or as a bad merger tactic.
- A **hostile merger** is a merger transaction that the target firm's management does not support. The acquiring company is forced to try to gain control of the firm by buying shares in the marketplace. Varieties of defensive tactics are available to stop the hostile takeover attempts.
- A **Pac-Man defense** is a threat to undertake a hostile takeover of the prospective combinor.

- A **poison pill** is a takeover defense in which an acquiring firm issues new securities that give its current shareholders certain rights that become effective when a takeover is attempted; these rights make the target firm less desirable to a hostile acquirer. The poison pill action will seriously damage a target company if it is acquired by a hostile firm. It may involve an amendment of the articles of incorporation or bylaws to make it more difficult to obtain stockholders' approval for a hostile takeover. A poison pill is a shareholder rights plan aimed at discouraging or preventing hostile takeovers. Typically, the poison pill provides that when a hostile suitor acquires more than a certain percentage of a company's stock, other shareholders receive share purchase rights designed to dilute the suitor's holdings and make the acquisition prohibitively expensive. Here the poison pill is a bad merger tactic and a takeover defense.
- A **poison put** is a variation of the poison pill as it forces a firm to buy its securities (e.g., stocks) back at some set price. Here the poison put is a bad merger tactic.
- A **scorched earth strategy** is the disposal of assets either by sale or by spin-off to stockholders of one or more profitable business segments. Target firms often sell or threaten to sell their major assets (i.e., **crown jewels**) when faced with a hostile takeover threat. This tactic often involves a lockup (another name for a scorched earth strategy).
- A **lockup** is an option granted to a friendly suitor (e.g., a white knight) giving it the right to purchase stock or some of the major assets (e.g., crown jewels) of a larger firm at a fixed price in the event of an unfriendly takeover.
- A **shark repellent** is any tactic (e.g., poison pill) designed to discourage hostile or unwanted merger offers. It may involve acquisition of substantial amounts of outstanding common stock in exchange for treasury stock or for retirement of stock, or incurring of substantial long-term debt in exchange for the outstanding common stock.
- A **white knight** occurs when the target firm finds a friendly new acquiring firm that is more acceptable to its management than the initial hostile acquirer. Then the white knight and the target firm together can compete to take over the acquiring firm. The friendly firm is the white knight. This it is a good merger tactic.
- A **greenmail** occurs when a target firm repurchases, through private negotiations, a large block of stock at a premium price from one or more shareholders to end a hostile takeover attempt by those shareholders. The target companies pay the greenmail to end the threat of a takeover attempt. Here greenmail is a bad merger tactic.
- A **white mail** occurs when white knights or others are granted exceptional merger terms or otherwise well compensated. Here the white mail is a good merger tactic.
- A **leveraged buyout** (LBO) is a transaction in which a firm's publicly owned stock is bought up in a mostly debt-financed tender offer. The result is a privately owned and highly leveraged firm. It is an example of a financial merger.
- An **initial public offering** (IPO) or **going public** means that a privately owned firm is offering its shares to public ownership the first time. After an IPO, the public owns a part of the private firm for the first time.
- A **holding company** is a corporation that has voting control of one or more other corporations.

Key terms, actions, and tactics used in a *friendly merger* include: up front, honest, and amicable communication, and use of white knight and white mail as needed and only after thorough research, keen observations, expert advice, and detailed analysis and evaluations are performed.

Key terms, actions, and tactics used in a *hostile merger* include: tender offer, poison pill, poison put, shark repellent, scorched earth, greenmail, Pac-Man defense, and golden parachute.

Key terms, actions, and tactics used in a *divestiture* include: scorched earth, selling crown jewels, lockup, spin-offs, and selling a profitable division and setting it up as a new company for existing stockholders.

(vii) Similarities and Differences Between Acquisitions and Divestitures

Most companies actively perform acquisition (includes both M&A) activities in buying new businesses or assets and passively perform selling some of their existing businesses and assets for glamour, recognition, and status to a name a few reasons. There is nothing wrong with selling underperforming and money-losing businesses or assets that do not fit well with a company's core business and that could prove more valuable to other firms. This is because both acquisitions and divestitures have the same goal of increasing returns to shareholders (e.g., wealth, profit, and stock price maximization, and all leading to the ultimate goal of maximizing shareholders' value).

- Acquisitions need a team approach to perform buy-side activities in a systematic, disciplined, and structured manner.
- Divestitures need a team approach to perform sell-side activities in a systematic, disciplined, and structured manner.
- Both require the same amount of planning, time, effort, and analysis from a strategic, operational, technical, and cultural viewpoints before making a final decision.
- Both should perform a fit-gap analysis to determine what new business or assets to be acquired and what existing businesses or assets should be disposed off, either in whole or in part. This fit-gap analysis should follow the core business objectives and goals.
- Both have the same problem of buying or selling assets at the wrong time, at the wrong price, to a wrong party, and in a wrong manner.
- Both operate on the assumption that there is always a buyer and a seller available to start and complete a business transaction.
- Acquisitions need an integration plan and approach to combine the new business with the current business.
- Divestitures need a deintegration plan and approach to separate the sold business from the current business.
- Both have a negative impact on current employees in terms of their job performance levels. Job motivation levels, pay levels, job security needs; pension and retirement benefits; medical and health care benefits; severance pay amounts, outplacement services, and job seniority levels.
- In divestitures, each potential buyer can become a potential competitor later on.
- In acquisitions, a normal due diligence review should be conducted by a buyer through the seller' eyes to quantify risks, opportunities, costs, profits, and revenue synergies for potential sellers.
- In divestitures, a reverse due diligence review should be conducted by a seller through the buyer's eyes to quantify risks, opportunities, costs, profits, and revenue synergies for potential buyers.

- Both sides should bring a win-win attitude to the negotiating table during acquisition and divestiture discussions. However, the real outcome is not known until after the acquisition or divestiture is fully completed and has operated for some time.

7.2 Managerial Accounting

The scope of managerial accounting (MA) topics include a discussion of costing systems; cost concepts; relevant costs; cost-volume-profit (CVP) analysis; transfer pricing; responsibility accounting; and operating budgets. In addition, general concepts in MA are briefly presented and compared with FA where necessary.

(a) Managerial Accounting: General Concepts

One can think of MA and FA topics as the two sides of a coin because one side provides information to the other side, and each side shares some common information with each other. For example, internal managers and executives share and use some FA reports, such as balance sheets, income statements, statements of cash flows, and other customized financial reports. Some activities are similar between MA and FA (e.g., record keeping) while activities (e.g., decision making) are different.

- The major focus of MA is satisfying the internal needs of an organization by helping the board of directors, executives, managers, and employees. The focus of FA is meeting the external needs of an organization by helping investors, owners, creditors, governmental agencies, suppliers and vendors, and labor unions through publishing financial statements and filing tax reports.
- Most MA decisions are future oriented (i.e., focusing on incremental revenues, costs, and profits) instead of past oriented (historical costs, revenues, and profits) as in FA.
- Inventory valuation methods are different between MA and FA, thus affecting the value of inventory assets, costs, and net incomes. FA uses GAAP whereas MA does not use GAAP. GAAP offers more flexibility to MA than the FA.
- MA looks at incremental and differential costs, revenues, and profits prior to making current decisions
- MA considers opportunity costs (implicit costs) in decision making; these costs are not recorded in FA transactions.
- MA separates relevant costs from irrelevant costs, handles transfer pricing issues between departments and divisions, and fosters responsibility accounting in making managers and executives more accountable to their actions or inactions.
- Both MA and FA have a similar policy in terms of financing long-term assets with long-term liabilities and financing short-term assets with short-term liabilities. It is called maturity matching. Any misuse of this matching policy can lead to financial volatility and to loss of profitability and solvency.
- MA helps managers and executives understand the basic cost concepts and their behaviors (e.g., period costs versus product costs; variable costs versus fixed /mixed costs; direct costs versus indirect costs; short-run costs versus long-run costs; avoidable costs versus unavoidable costs; controllable costs versus uncontrollable costs; discretionary costs

versus nondiscretionary costs, and committed costs versus uncommitted costs) when establishing long-term prices for products and services and after considering changes in production volumes, sales volumes, and workforce volumes and their effects on profit and growth levels.

- MA experiments with or researches new costing systems for products and services, such as activity-based or target-based costing methods to determine the true cost of a product and service and to see how such costs can be decreased and profits can be increased without decreasing quality.
- MA works with technologies and innovations, such as flexible manufacturing systems, computer-aided manufacturing, bar-coding systems, point-of-sale (POS) terminals, robotics, just-in-time (JIT) philosophies, lean production methods, total quality management (TQM) principles, Six Sigma tools, ISO standards, and cellular manufacturing systems.
- MA's goal is to identify and remove non-value-adding activities and waste from value-adding activities in manufacturing and services to conserve resources, decrease costs, and increase profits.
- MA uses both capital budgeting and operating budgets as control devices in managing cash inflows and cash outflows and in estimating cash needs for both the short and the long term.
- MA deals with nonprogrammed and nonroutine decisions for managers and executives. These decisions include:
  - Building a new manufacturing plant, warehouse, or office
  - Handling mergers, acquisitions, and divestitures
  - Introducing new products and services
  - Divesting an existing product or service
  - Making lease-or-buy decisions
  - Analyzing make-or-buy decisions
  - Entering new markets with new or existing distribution channels or exiting from such markets and channels
  - Setting long-term pricing policies (i.e., price leader or follower)
  - Deciding between insourcing or outsourcing of products and services
  - Addressing workforce staffing, planning, and diversity management issues
  - Understanding cost of compliance versus costs of noncompliance with laws and regulations
  - Abandoning a specific nonperforming product/product line or service or closing a money-losing department or division
  - Setting short-term prices for certain products or services based on a one-time big order from a major customer at least to recover variable costs, increase contribution margins (CMs), ignoring long-term fixed costs, all of which can increase short-term profits

In summary, MA concepts and decisions are nonsequential, unstructured, nonprogrammed, and nonroutine in nature and are handled mostly by high-level management. The reverse is not true with FA.

(b) Costing Systems

Product cost control systems can be viewed in terms of target costing and traditional costing a product.

(i) Target Costing

Target costing is a better way of controlling a product's cost. A target cost is the allowable amount of cost that can be incurred on a given product and still earn the required profit margin. It is a market-driven cost in which cost targets are set by considering customer requirements and competitive environment. Cost targets are achieved by focusing and improving both process design and product design. Market research indicates the target price customers are willing to pay.

$$\text{Target price} - \text{Profit margin} = \text{Target cost}$$

The need for target costing arises due to sophisticated customers demanding better-quality products with more features and functions at an affordable price. This is made real by aggressive competitors who are willing to take risks and provide a product at a target price with the hope of achieving efficiencies in cost management and production operations.

Target costing is not the same as design to cost or design for manufacturability, which are issues for engineering and manufacturing management respectively. Target costing integrates strategic business planning with cost/profit planning. To achieve this integration, a target-costing system requires cross-functional teams to take ownership and responsibility for costs. These teams consist of representatives from finance/accounting, marketing, engineering, manufacturing, and other functions.

(ii) Traditional Costing

Traditional costing systems use a cost-plus approach, where production costs are first estimated, then a profit margin is added to it to obtain a product price that the market is going to pay. If the price is too high, cost reductions are initiated. Traditional costing systems are cost-driven approaches where customer requirements and competitive environment are not considered.

$$\text{Traditional production cost} + \text{Profit margin} = \text{Traditional product price}$$

The cost to manufacture a product is necessary for external reporting (e.g., inventory valuation and COGS determination) and internal management decisions (e.g., price determination, product mix decisions, and sensitivity analysis). One of the goals of cost accounting is to provide information for management planning and control and determination of product or service costs. This is achieved through the accumulation of costs by department and/or by product. Although the terminology differs between manufacturing and service industries, the principles of cost accounting are the same.

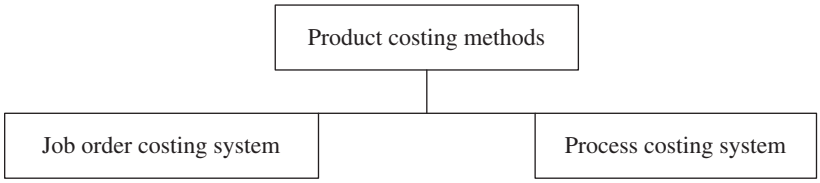
Two methods exist to accumulate product costs: job order costing system and process (operations) costing system. Both methods help management in planning and control of business operations. A job order cost system provides a separate record for the cost of each quantity of product that passes through the factory. A job order cost system is best suited to industries that manufacture custom goods to fill special orders from customers or that produce a high variety of products for stock (job shops). Under a process cost system, costs are accumulated for each of the departments or processes within the factory. A process cost system is best suited for manufacturers of

units of products that are not distinguishable from each other during a continuous production process (e.g., oil refineries and food processing).

TRADITIONAL COST SYSTEMS VERSUS TARGET COST SYSTEMS

- Traditional cost systems are closed systems where the focus is on internal measures of efficiency. Suppliers are involved after the product is designed. Cost reduction is initiated after the fact based on product standards or budgets with the aim of reducing or eliminating waste and inefficiency. Costs determine price.
- Target cost systems are open systems where the focus is on external market demands. Suppliers are involved before the product is designed. Cost reduction is initiated before the fact based on continuous improvement opportunities with the aim of enhancing the product's design. Prices determine costs.

Exhibit 7.46 compares these two product cost systems.



Characteristics of job order costing system	Characteristics of process costing systems
Unlike (heterogeneous) products are manufactured.	Like (homogeneous) products are manufactured.
Products tend to be special and unique.	Products tend to be common and generic.
Costs are allocated to a specific unit or to a small batch of products or services.	Costs are allocated to a large number of units that proceed in a continuous fashion.
A production job retains its identity from start to finish.	A production job does not retain its identity due to by-products, joint products, and main products.
Costs are averaged (i.e., total costs divided by small number of units of production).	Costs are averaged (i.e., total costs divided by large number of units of production).
Only one work in process (WIP) account is involved, and units move from WIP to finished goods.	Several WIP accounts are involved, and units move from one department's WIP account to the next.
Costs are collected separately for each job.	Costs are collected separately for each process and then summed up.
Systems are complex and more expensive than in the process costing method.	Systems are simpler and less expensive than the job order costing method.
Examples include printing jobs and construction jobs.	Examples include oil refineries, food products, and soft drinks.

EXHIBIT 7.46 Comparison of Product Costing Methods

(iii) Activity-Based Costing

Activity-based costing (ABC) is a management system that focuses on activities as the fundamental cost objects and uses the costs of these activities as building blocks for compiling the costs of other cost objects. ABC helps management in controlling costs through its focus on cost drivers. ABC can provide more accurate product cost data by using multiple cost drivers that more accurately reflect the causes of costs. Inaccurate product cost information can lead to cross-subsidization of products. This results in systematic under-costing of products due to lower overhead rate. These cost drivers can be both non-volume-based as well as volume-based drivers.

KEY CONCEPTS TO REMEMBER: Activity-Based Costing

- The key focus of ABC is on activities, not on products. This is in line with the philosophy of executives in managing costs. The scope of activities may range from start to finish for a product or service (i.e., from R&D to customer service).
- If the manufacturing process is described as machine-paced, then machine hours should be used as the cost driver.
- If the manufacturing process is described as labor-paced, then direct labor hours should be used as the cost driver.
- If direct labor is a small percentage (e.g., 5%) of total manufacturing costs, it should be regarded as a part of indirect costs, not direct costs.
- The ABC can be a part of a job-costing or process-costing system.

ABC builds the cost of a product from the bottom up for all activities involved (A1 through A*n*) in all departments (D1 through D*n*) in a manufacturing function yielding to inventoriable cost. The full cost of a product is obtained similarly by adding costs for functions. Manufacturing and nonmanufacturing (e.g., R&D, product design, marketing, customer service) costs are accumulated for each activity as a separate cost object. The costs collected at each cost object can be variable costs of the activity or both variable and fixed costs of the activity.

(A) Benefits of Activity-Based Costing System Major benefits of an ABC system are listed next.

- Better cost control
- Accurate product cost information
- Lower information processing costs
- Individual costs allocated to products via several cost drivers
- Better make-or-buy decisions
- Focus on activities where costs are incurred and accumulated instead of products

(B) When to Use an Activity-Based Costing System An ABC system should be used in companies that have these characteristics:

- High overhead costs
- A widely diverse range of products and operating activities

- Wide variation in number of production runs and costly setups
- The accounting system las behind the production system's advancements

(C) Comparison of a Traditional Accounting System with an Activity-Based Costing System A better appreciation of an ABC system can be made when it is compared with the traditional, typical accounting system (see Exhibit 7.47).

Traditional accounting system	Activity-based costing system
Functions are divided into departments.	Departments are divided into activities.
The system fails to highlight the interrelationships among activities in different departments or functions.	The system highlights the interrelationships among activities in different departments or functions.
Accountants need not possess interpersonal skills to interact with production staff.	Accountants need to possess interpersonal skills to interact with production staff.
Accountants need not become knowledgeable in production operations.	Accountants need to become knowledgeable in production operations.
One or a few indirect cost pools are used for each department or whole plant.	Many indirect cost pools are used because there are many activity areas.
Indirect cost application bases are often financial, such as direct labor costs or direct material costs.	Indirect cost application bases are often nonfinancial variables, such as the number of parts in a product or hours of test time.
Indirect costs are allocated to products using a single overhead rate.	Indirect costs are allocated to products using multiple cost drivers, preferably the same as the indirect cost application bases.

EXHIBIT 7.47 Comparison of Traditional Accounting System with Activity-Based Costing System

(iv) Standard Costing

Standard costs are predetermined costs or estimated costs requiring a start-up investment to develop them. Ongoing costs for maintenance of standards can be lower than for an actual-cost system. Standard costs should be attainable and are expressed on a per-unit basis. Without standard costs, there is no flexible budgeting system since the latter is developed at different volumes of production using standard costs per unit.

Standard costs, flexible budgets, and standards are equally applicable to manufacturing and nonmanufacturing firms. Standard costs and flexible budgets are interrelated. A flexible budget is a budget that is adjusted for changes in the unit level of the cost driver or revenue driver. In a standard cost system, the concept of a flexible budget is key to the analysis of variances.

A powerful benefit of standard costing is its feedback mechanism where actual costs are compared with standard costs resulting in variances. This feedback helps users to explore better ways of adhering to standards, modifying standards, and accomplishing production goals. Standard costs can be developed for material, labor, and overhead. One drawback of a standard cost system is that actual direct material costs and actual direct labor costs cannot be traced to individual products.

STANDARD COST VERSUS BUDGETED COST

- Standard cost refers to the cost of a single unit of output (e.g., $50 per unit).
- Budgeted cost refers to a total amount ($500,000 at 10,000 units).
- A standard amount and a budgeted amount are the same when standards are attainable.

Major purposes of standard costs are listed next, in decreasing order of importance.

- Cost management
- Price-making policy
- Budgetary planning and control
- Financial statement preparation
- Lower record-keeping costs

Line management is responsible for standard setting and the budget-development process. The accounting department, which is a staff function, is responsible for expressing the physical standard in monetary terms, for coordinating the budgeting process throughout the firm, and for reporting operating performance in comparison with standards and budgets.

Standards help in evaluating the performance of responsibility centers. Most recently established standards should be used in variance analysis. Variances—differences between standards and actuals—can be developed, reported, and tracked for control purposes in a number of ways, as shown in Exhibit 7.48.

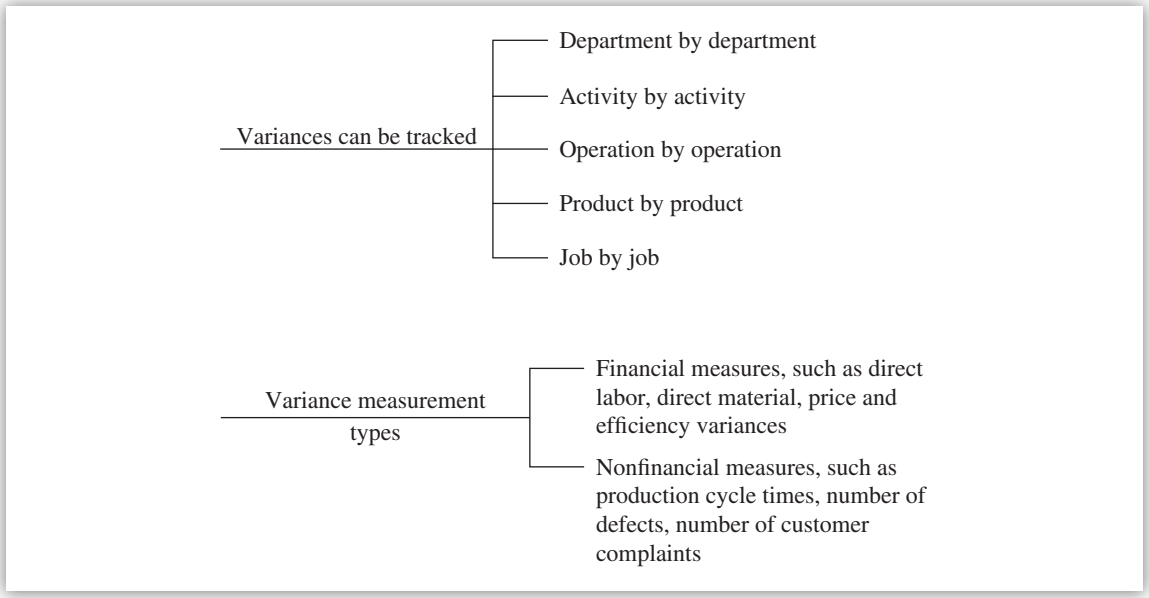


EXHIBIT 7.48 Different Ways of Tracking and Measuring Variances

Organizations are moving away from financial measures to nonfinancial measures for better focus on the problem at hand. For example, one reason for moving away from direct labor as

a measurement of variance is its minor role in total cost for firms with automated production operations.

(A) Types of Standards Two concepts prevail in standards: perfection (ideal or theoretical) standards and currently attainable standards. Their features are shown in the Exhibit 7.49.

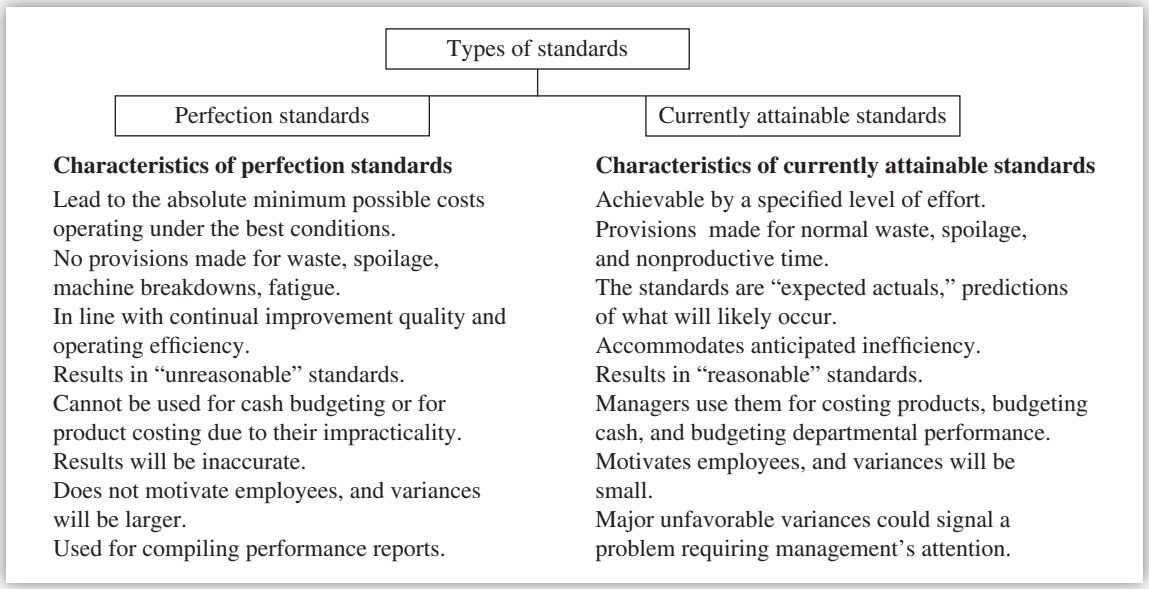


EXHIBIT 7.49 Characteristics of Standards

(B) Types of Variances In general, **price variance** is the difference between actual unit prices and budgeted unit prices multiplied by the actual quantity of goods sold, used, or purchased.

$$\text{Price variance} = (\text{Actual unit price} - \text{Standard unit price}) \times \text{Actual inputs purchased}$$

Companies that use fewer suppliers and longer-term contracts are less likely to have significant material price variances. This is because contracts specify unchanging prices for fixed time spans and the buying firm has leverage against the selling firm.

Companies that use several suppliers and short-term contracts are more likely to have significant material price variances. This is because contracts are frequently changed or canceled and the buying firm has little or no leverage against the selling firm.

The purchasing manager is responsible for the material price variance and he can help control it by:

- Getting many price quotations.
- Buying in economical lot sizes.
- Taking advantage of cash discounts.
- Selecting the most economical means of material delivery.

These could result in a favorable material price variance, depending on how material standards are set.

Due to labor union contracts, labor price variance is relatively insignificant since management knows the future labor rates, unlike material prices.

In general, **efficiency variance** is of two types: material efficiency and labor efficiency. Possible reasons for material efficiency variances are listed next.

- Quality of materials
- Workmanship
- Choice of materials
- Mix of materials
- Incorrect standards

Efficiency variance is the difference between the quantity of actual inputs used and the quantity of inputs that should have been used multiplied by the budgeted price.

$$\text{Efficiency variance} = (\text{Inputs actually used} - \text{Inputs that should have been used}) \times \text{Standard unit price of inputs}$$

The factory supervisor is responsible for the efficiency variance. Efficiency variance is quantity or usage variance with respect to direct materials.

Specifically, **direct materials variance** is of two types: price and quantity. The price variance is actual price paid per unit of input (AP) minus standard price established per unit of input (SP) multiplied by actual quantity of input used in production (AQ).

$$\text{Direct materials price variance} = (AP - SP) \times AQ$$

The materials price variance is unfavorable if AP is greater than SP and favorable if AP is less than SP.

The quantity variance is actual quantity of input used in production (AQ) minus standard quantity of input that should have been used in production (SQ) multiplied by standard price established per unit of input (SP).

$$\text{Direct materials quantity variance} = (AQ - SQ) \times SP$$

The materials quantity variance is unfavorable if AQ is greater than SQ and favorable if AQ is less than SQ.

Specifically, **direct labor variance** is of two types: rate and efficiency. The rate variance is actual price paid per unit of input (AP) minus standard price established per unit of input (SP) multiplied by actual quantity of input used in production (AQ).

$$\text{Direct labor rate variance} = (AP - SP) \times AQ$$

The labor rate variance is unfavorable if AP is greater than SP and favorable if AP is less than SP.

The efficiency variance is actual quantity of input used in production (AQ) minus standard quantity of input that should have been used in production (SQ) multiplied by standard price established per unit of input (SP).

$$\text{Direct labor efficiency variance} = (AQ - SQ) \times SP$$

The labor efficiency variance is unfavorable if AQ is greater than SQ and favorable if AQ is less than SQ.

Specifically, **overhead variance** is of four types: (1) spending variance, (2) efficiency variance, (3) budget variance, and (4) volume variance. Variances (1) and (2) are part of variable overhead variances while variances (3) and (4) are part of fixed overhead variances.

$$\text{Spending variance} = \text{Actual variable overhead} - (\text{Actual hours} \times \text{Budget rate})$$
$$\text{Efficiency variance} = \text{Budget rate} \times (\text{Actual hours} - \text{Standard hours})$$

The budget variance is sometimes called the fixed overhead spending variance. It is calculated as the difference between actual fixed costs and budget fixed costs.

The volume variance is sometimes called the idle capacity variance. This is computed as Budget fixed cost – (Standard hours allowed for actual output at standard rate).

Example Calculation of Variances

Example 1

A manager prepared the following table by which to analyze labor costs for the month:

Actual hours at actual rate	Actual hours at standard rate	Standard hours at standard rate
$10,000	$9,800	$8,820

What variance was $980? It is the labor efficiency variance, which is the difference between actual and standard hours multiplied by standard wages. That is, $9,800 – $8,820 = $980.

Example 2

A firm's budget showed planned sales of 20,000 units at a $20 CM each, or $400,000. Actual sales totaled 21,000 units. There were no variable cost variances. What was the sales volume variance for the period? It is $20,000, as shown below.

The sales volume variance is the difference between actual results (21,000 units) and planned results (20,000 units) at planned CM ($20), or $20,000.

Example 3

The next exhibit reflects a summary of performance for a single item of a retail store's inventory for the month ended April 30, 20X2.

	Actual results	Flexible budget variances	Flexible budget	Static (master) budget
Sales (units	11,000		11,000	12,000
Revenue (sales)	$208,000	$12,000 U	$220,000	$240,000
Variable costs	121,000	11,000 U	110,000	120,000
Contribution margin	$121,000	$23,000 U	$110,000	$120,000
Fixed costs	72,000		72,000	72,000
Operating income	49,000	$23,000 U	$38,000	$48,000

What is the sales volume variance? It is $10,000 U, as shown below. Sales volume variance is defined as the difference between the flexible-budget amounts and the static (master)-budget amounts ($38,000 – $48,000 = $10,000 U). U is unfavorable.

KEY CONCEPTS TO REMEMBER: Price and Efficiency Variance

- A manager has less control over price variance because of outside influences. Variance is the difference in price multiplied by actual inputs purchased.
- A manager has better control over efficiency variance because the quantity of inputs used is affected by factors inside the firm. Efficiency variance is the difference in quantity multiplied by the standard unit price.
- Price and efficiency variances are either written off immediately to COGS or prorated among the inventories and COGS.

A performance measurement and reward system for a firm should emphasize total organizational objectives, not individual departments' variances. The goal is to reduce the total costs of the company as a whole, not price variance or efficiency variance (i.e., single performance measure).

Although labor rates are known from union contracts, unfavorable labor price variance can occur due to:

- The use of a single average standard labor rate for a given activity that requires different labor rates (the averaging effect).
- The assignment of a high-skilled worker earning more money to an activity that should have been assigned to a less-skilled worker earning less money.

The control of direct labor is more important to firms with less automation and less important to firms with more automation. The source documents for variance reports are time tickets showing the actual time used. Codes are used to indicate the departmental responsibility and causes of the variance. Employee absenteeism can affect labor efficiency.

Variance analysis should be subjected to the same cost/benefit test as any other managerial decision. No fixed guidance can be given as to how much unfavorable or favorable variance ought to be analyzed. However, it is important to separate variances caused by random events (uncontrollable) from variances that are controllable. Random variances are attributable to chance rather than to management's implementation decisions.

KEY CONCEPTS TO REMEMBER: What Is a Standard?

- A standard is not a single acceptable measure.
- A standard is a range of possible acceptable outcomes.
- Variances are expected to fluctuate randomly within some normal limits. A random variance per se is within this range and requires no corrective action. Only nonrandom variance requires corrective action by management.

(C) Effects of Variance Prorations GAAP and income tax laws require that financial statements show actual costs of inventories and COGS. Consequently, variance prorations are required if

they result in a material change in inventories or operating income. Variance is the difference between actual costs and standard costs. A good benefit of proration is that it prevents managers from setting standards aimed at manipulating income. By setting loose standards, managers can bring the resulting favorable variance into current income. If managers do not have to prorate variances, how they set standards can more easily affect a year's operating income. The relevant questions are listed next.

- **How should variances occurring during the first stages of new operations be accounted for?** Standards might initially be set at a loose level to allow for start-up inefficiencies, and later they should be tightened. If the standards are currently attainable, variances should be carried forward as assets and written off in future periods.
- **How should variances be prorated?** First, a decision should be made whether proration should occur, and it usually depends on whether the variances are material in amount.

Decision Rules to Handle Variances:

1. Immaterial variances should be written off immediately and adjusted to COGS.
2. Material variances should be prorated as follows: (a) to affect current incomes by posting to COGS and income accounts, (b) to affect inventories by apportioning among WIP, finished goods, and COGS.

Some contend that variances are measures of inefficiency and should be completely written off to the accounting period instead of being prorated among inventories and COGS. They argue that inventory costs will be more representative of desirable and attainable costs.

KEY CONCEPTS TO REMEMBER: Variances

- Variance proration tends to carry costs of inefficiency as assets.
- Variances need not be prorated to inventories as long as standards are currently attainable.
- If ideal or obsolete standards are used, variances should be split: (1) The portion of the variance that reflects departures from currently attainable standards should be written off as period costs, and (2) the portion that does not reflect departure from currently attainable standards should be prorated to inventories and COGS.

Adjustments to inventory accounts are made to satisfy external reporting requirements. The adjustments include:

- **Converting** a variable-costing inventory valuation to absorption-costing valuation.
- **Prorating variances.** The journal entry to accomplish this adjustment would be to **debit** the finished goods inventory adjustment account and to **credit** either the fixed factory overhead or cost variance accounts (e.g., direct material price variance).

(D) Reporting of Variances Interim reporting of variance differs among companies. Some firms write off all variances monthly or quarterly to COGS while others prorate the variances among inventories and COGS. Most firms follow the same reporting practices for both interim and annual financial statements.

Interim overhead variances are often called "planned" variances and are deferred. These variances include direct material price variances and factory overhead production volume variances. The rationale is that these variances are expected to disappear by the end of the year through the use of averaging as costs are applied to the product. The "unplanned," unanticipated, underapplied, or overapplied overhead should be reported at the end of an interim period following the same procedures used at the end of a fiscal year (according to APB Opinion 28).

UNDERAPPLIED VERSUS OVERAPPLIED MANUFACTURING OVERHEAD

- If underapplied manufacturing overhead is carried forward during the year, it would appear on an interim balance sheet as a current asset, a prepaid expense.
- If overapplied manufacturing overhead is carried forward during the year, it would appear on an interim balance sheet as a current liability, a deferred credit.

(c) Cost Concepts

Various cost concepts are introduced in this section along with their specific meanings, application, behavior with changes in sales and production volumes, and estimation methods.

(i) Absorption and Variable Costing Methods

The COGS, which is larger than all of the other expenses combined in a product cost, can be determined under either the absorption costing or variable costing method.

Under **absorption costing**, all manufacturing costs are included in finished goods and remain there as an inventory asset until the goods are sold. Management could misinterpret increases or decreases in income from operations due to mere changes in inventory levels to be the result of business events, such as changes in sales volume, prices, or costs. Absorption costing is necessary in determining historical costs for financial reporting to external users and for tax reporting.

Variable costing may be more useful to management in making decisions. In variable costing (direct costing), the cost of goods manufactured is composed only of variable manufacturing costs—costs that increase or decrease as the volume of production rises or falls. These costs are the direct materials, direct labor, and only those factory overhead costs that vary with the rate of production. The remaining factory overhead costs, which are fixed or nonvariable costs, are generally related to the productive capacity of the manufacturing plant and are not affected by changes in the quantity of product manufactured. Thus the fixed factory overhead does not become a part of the cost of goods manufactured but is treated as an expense of the period (period cost) in which it is incurred.

The income from operations under variable costing can differ from the income from operations under absorption costing. This difference results from changes in the quantity of the finished goods inventory that are caused by differences in the levels of sales and production.

The following decision rules apply.

- If units sold are less than units produced, then variable costing income is less than absorption costing income.
- If units sold are greater than units produced, then variable costing income is greater than the absorption costing income.

Many accountants believe that the variable costing method should be used for evaluating operating performance because absorption costing encourages management to produce inventory. This is because producing inventory absorbs fixed costs and causes the income from operations to appear higher. In the long run, building inventory without the promise of future sales may lead to higher handling, storage, financing, and obsolescence costs.

(ii) Management's Use of Absorption and Variable Costing Methods

Management's use of absorption costing and variable costing includes controlling costs, pricing products, planning production, analyzing market segments (sales territory and product profitability analysis), and analyzing the CM. Preparing comparative reports under both concepts provides useful insights.

(A) Controlling Costs All costs are controllable in the long run by someone within a business, but they are not all controllable at the same level of management. For example, plant supervisors, as members of operating management, are responsible for controlling the use of direct materials in their departments. They have no control, however, of insurance costs related to the buildings housing their departments. For a specific level of management, **controllable costs** are costs that can be influenced by management at that level, and **noncontrollable costs** are costs that another level of management controls. This distinction is useful in fixing the responsibility for incurring costs and for reporting costs to those responsible for their control.

Variable manufacturing costs are controlled at the operating level. If the product's cost includes only variable manufacturing costs, operating management can control these costs. The fixed factory overhead costs are normally the responsibility of a higher level of management. Fixed factory overhead costs that are reported as a separate item in the variable costing income statement are easier to identify and control than when they are spread among units of product, as they are under absorption costing.

As in the case with the fixed and variable manufacturing costs, the control of variable and fixed operating expenses is usually the responsibility of different levels of management. Under variable costing, the variable selling and administrative expenses are reported separately from the fixed selling and administrative expenses. Because they are reported in this manner, both types of operating expenses are easier to identify and control than is the case under absorption costing.

(B) Pricing Products Many factors enter into determining the selling price of a product. The cost of making the product is clearly significant. Microeconomic theory states that income is maximized by expanding output to the volume where the revenue realized by the sale of an additional unit (marginal revenue) equals the cost of that unit (marginal cost). Although the degree of accuracy assumed in economic theory is rarely achieved, the concepts of marginal revenue and marginal cost are useful in setting selling prices.

In the short run, a business is committed to its existing manufacturing facilities. The pricing decision should be based on making the best use of such capacity. The fixed costs cannot be avoided, but the variable costs can be eliminated if the company does not manufacture the product. The selling price of a product, therefore, should at least be equal to the variable costs of making and selling it. Any price above this minimum selling price contributes an amount toward covering fixed costs and providing income. Variable costing procedures yield data that emphasize these relationships.

In the long run, plant capacity can be increased or decreased. If a business is to continue operating, the selling prices of its products must cover all costs and provide a reasonable income. Hence,

in establishing pricing policies for the long run, information provided by absorption costing procedures is needed. The results of a research study indicated that the companies studied used absorption costing in making routine pricing decisions. However, these companies regularly used variable costing as a basis for setting prices in many short-run situations.

(C) Planning Production Planning production also has both short-run and long-run implications. In the short run, production is limited to existing capacity. Operating decisions must be made quickly before opportunities are lost. For example, a company manufacturing products with a seasonal demand may have an opportunity to obtain an off-season order that will not interfere with its production schedule or reduce the sales of its other products. The relevant factors for such a short-run decision are the additional revenues and the additional variable costs associated with the off-season order. If the revenues from the special order will provide a CM, the order should be accepted because it will increase the company's income from operations. For long-run planning, management must also consider the fixed costs.

(D) Analyzing Market Segments Market analysis is performed by the sales and marketing function in order to determine the profit contributed by market segments. A **market segment** is a portion of business that can be assigned to a manager for profit responsibility. Examples of market segments include sales territories, products, salespersons, and customer distribution channels. Variable costing can provide significant insight to decision making regarding such segments.

(E) Analyzing Contribution Margins Another use of the CM concept to assist management in planning and controlling operations focuses on differences between planned and actual CMs. However, mere knowledge of the differences is insufficient. Management needs information about the causes of the differences. The systematic examination of the differences between planned and actual CMs is termed **contribution margin analysis**.

Since CM is the excess of sales over variable costs, a difference between the planned and actual CM can be caused by an increase or decrease in the amount of either sales or variable costs. An increase or decrease in either element may in turn be due to an increase or decrease in the (1) number of units sold (quantity factor) or (2) unit sales price or unit cost (unit price or unit cost factor). The effect of these two factors on either sales or variable costs may be stated as follows:

1. **Quantity factor.** The effect of a difference in the number of units sold, assuming no change in unit sales price or unit cost. The quantity factor is the difference between the actual quantity sold and the planned quantity sold, multiplied by the planned unit sales price or unit cost.
2. **Unit price factor or unit cost factor.** The effect of a difference in unit sales price or unit cost on the number of units sold. The unit price or unit cost factor is the difference between the actual unit price or unit cost and the planned unit price or unit cost, multiplied by the actual quantity sold.

(iii) Technical Aspects of Absorption and Variable Costing Methods

An understanding of the inventory costing method is important for several reasons, such as:

- Measuring product costs and inventories.
- Determining income.
- Deciding between making or buying a product.

- Setting prices.
- Planning product mix to produce or sell.

Two major methods of inventory costing are absorption costing and variable costing (see Exhibit 7.50), and they differ in whether fixed manufacturing overhead is an inventoriable cost (i.e., whether such overhead is included in the inventory or not). Other names used for fixed manufacturing overhead are fixed factory overhead and indirect manufacturing cost.

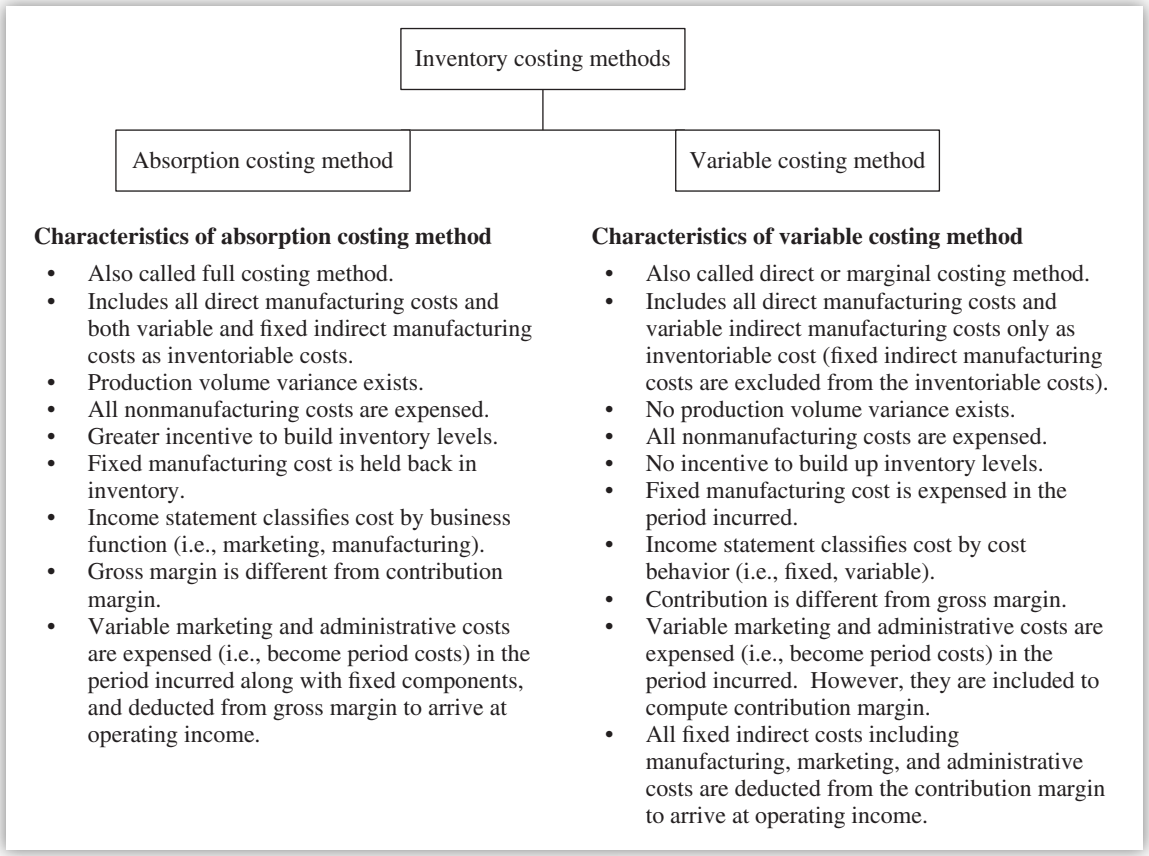


EXHIBIT 7.50 Two Major Methods of Inventory Costing

OPERATING INCOME UNDER THE ABSORPTION AND VARIABLE COSTING METHODS

Absorption costing method		**Variable costing method**	
Sales	$xxx	Sales	$xxx
Less variable manufacturing costs	xxx	Less variable manufacturing cost of goods sold	xxx
Less fixed manufacturing costs	xxx	Less variable marketing costs	xxx
Deduct ending inventory	xxx	Less variable administrative costs	xxx
Equals **gross margin**	xxx	Total variable costs	xxx
		Contribution margin	xxx
Deduct total marketing and administrative costs including variable costs	xxx	Deduct all fixed costs	xxx
Operating income	xxx	Operating income	xxx

The difference in operating income between these two methods arises from the difference in the amount of inventories. The CM and GM highlight the conflict of the underlying concepts of variable cost and absorption cost. Both methods can operate in conjunction with actual, normal, or standard costing systems.

The arguments for and against variable costing method are listed next.

Argument For
Fixed portion of factory overhead is relevant to overall plant capacity, not to the production of a specific product. Hence, the focus should be on all variable costs.

Argument Against
Inventories should contain fixed costs in addition to variable costs since both are needed to produce goods. Hence, all costs should be inventoried.

KEY CONCEPTS TO REMEMBER: Relationships between Variable Costing and Absorption Costing Methods

- If inventories increase during a period, the variable costing method will generally report less operating income than will the absorption costing method.
- If inventories decrease, the variable costing method will report more operating income than the absorption costing method.
- The differences in operating income are due solely to moving fixed overhead in and out of inventories.

  Absorption costing operating income – Variable costing operating income = Fixed overhead in ending inventory in absorption cost – Fixed overhead in beginning inventory in absorption costing
- The difference between variable costing and absorption costing incomes is a matter of timing. Under the variable costing method, fixed overhead is expensed in the period incurred. Under the absorption costing method, fixed overhead is inventoried and is expensed when the related units are sold.
- Under the variable costing method, operating income is drawn by fluctuations in sales volume. Operating income should increase as sales increase and vice versa. Operating income rises at the rate of the CM per unit. This dovetails precisely with CVP analysis, and the breakeven point (BEP) can be calculated easily. There are no temptations to manipulate income.
- Under the absorption costing method, both sales volume and production volume drive the operating income. Changes in inventory levels and choice of production schedule and volume can dramatically affect income. There are great temptations to manipulate income.
- Under the absorption costing method, it is possible to report a lower operating income even though sales volume increased due to the unusually large amounts of fixed overhead being charged to a single accounting period.
- If the number of units produced exceeds the number of units sold, ending inventory increases. Since absorption defers some fixed overhead in the increased ending inventory, absorption costing income is generally higher than variable costing income.
- A manager whose performance bonus is based on absorption costing income could increase production levels to obtain favorable production volume variance by hiding fixed overhead expenses

as inventoriable costs in order to increase income. A manager can also choose to decrease absorption costing income by decreasing inventory if he or she has met this year's targeted income. Thus, managers are tempted to make short-run decisions at the expense of long-run objectives of the organization.

- To balance the negative effects of the absorption costing method (such as buildup of inventory), a manager's performance should be based on both financial and nonfinancial criteria. Examples of nonfinancial performance criteria include meeting inventory levels, meeting product delivery dates, adhering to plant maintenance schedules, and meeting or exceeding product quality and customer service levels.
- Variable cost is not acceptable for tax or external financial reporting purposes. Variable cost is heavily used for internal management reporting.
- GAAP requires that all manufacturing overhead is inventoried. Some firms may choose not to include depreciation on factory equipment as part of inventory cost.
- The U.S. Internal Revenue Code requires that all manufacturing and some marketing, distribution, and administrative costs are included in inventory.

APPLICATION OF ABSORPTION AND VARIABLE COSTING METHODS

During the first year of operations, a company produced 275,000 units and sold 250,000 units. The following costs were incurred during the year:

Variable costs per unit	
Direct material	$ 15.00
Direct labor	10.00
Manufacturing overhead	12.50
Selling and administrative	2.50
Total fixed costs	
Manufacturing overhead	$ 2,200,000
Selling and administrative	1,375,000

What would be the difference between operating income calculated on the absorption (full) costing basis and on the variable (direct) costing basis?

a. Absorption costing operating income would be greater than variable costing operating income by $200,000.
b. Absorption costing operating income would be greater than variable costing operating income by $220,000.
c. Absorption costing operating income would be greater than variable costing operating income by $325,000.
d. Variable costing operating income would be greater than absorption costing operating income by $62,500.

Choice **(a)** is the correct answer. Absorption costing operating income will exceed variable costing operating income because production exceeds sales, resulting in a deferral of fixed manufacturing overhead in the inventory under absorption. The amount of difference is the fixed manufacturing overhead per unit ($2,200,000/275,000 = $8.00) times the difference between production and sales (275,000 – 250,000 = 25,000 units; this could also be stated as the inventory change in units). That is, $8.00 × 25,000 units = $200,000.

Choice (b) is incorrect. The reasoning is the same as response choice (a) except fixed manufacturing overhead per unit is calculated by using unit sales rather than production units ($2,200,000/250,000 = $8.80; $8.80 × 25,000 = $220,000).

Choice (c) is incorrect. The reasoning is the same as response choice (a) except all fixed costs treated as being inventoriable under absorption costing and production units used as the base [($2,200,000 + 1,375,000)/275,000 = $13.00; $13.00 × 25,000 = $325,000)].

Choice (d) is incorrect. This response assumes that the difference between variable and absorption costing is that variable selling and administrative costs are inventoriable for variable costing and not inventoriable for absorption costing; thus, a portion of the variable selling and administrative expenses would be deferred in the inventory, meaning variable operating income would exceed absorption operating income ($2.50 × 25,000 = $62,500).

(iv) Other Cost Concepts

The next list provides a brief description of cost concepts other than absorption or variable costs.

- **Actual costs.** The amounts determined on the basis of cost incurred for making a product or delivering a service to customers.
- **Average costs.** The total cost divided by the activity (i.e., number of units).
- **Budgeted costs.** Costs that were predetermined for managerial planning and controlling purposes.
- **Common costs.** Costs of facilities and services shared by several functional departments. These are costs incurred for the benefit of more than one cost objective.
- **Conversion costs.** A combination of direct labor costs, indirect material costs, and factory overhead. Assembly workers' wages in a factory are an example of conversion costs since their time is charged to direct labor.
- **Current costs.** Costs that represent fair market value at current date.
- **Direct costs.** Costs that can be directly identified with or traced to a specific product, service, or activity (e.g., direct labor and direct materials). In a manufacturing operation, direct material costs would include wood in a furniture factory since wood is a basic raw material of furniture. Direct labor costs are wages paid to workers.

  Other examples of direct costs include insurance on the corporate headquarters building since it is not a cost of production, depreciation on salespersons' automobiles, salary of a sales manager, commissions paid to sales personnel, and advertising and rent expenses.
- **Expired costs.** The portions of cost that are expensed. An expired cost is a period cost, and it is either an expense or a loss.
- **Fixed costs.** Costs that remain constant in total, but change per unit, over a relevant range of production or sales volume (e.g., rent and depreciation). A fixed cost is a unit cost that decreases with an increase in activity. It is constant in total but varies per unit in direct proportion to changes in total activity or volume. It is a cost that remains unchanged in total for a given period despite fluctuations in volume or activity as long as the production is within the relevant range. A fixed cost may change in total between different periods or when production is outside the relevant range. Therefore, unit fixed cost decreases as output increases at a given relevant range.

- **Full costs.** A combination of direct costs and a fair share of the indirect costs for a cost objective. Full costs refer to a unit of finished product. They consist of prime costs and overhead and are the entire sacrifice related to a cost objective.
- **Historical costs.** Costs incurred at the time of occurrence of a business transaction. They represent what costs were.
- **Indirect costs.** Costs that cannot be identified with or traced to a specific product, activity, or department (e.g., salaries, taxes, utilities, machine repairs). An example is a factory manager's salary. Another term for indirect costs is factory overhead. It consists of all costs other than direct labor and direct materials associated with the manufacturing process.
- **Joint costs.** Costs of manufactured goods of relatively significant sales values that are simultaneously produced by a process.
- **Long-run costs.** Costs that vary as plant capacity changes over a long period of time.
- **Marginal costs.** Costs to make an additional unit or the last unit. They are the incremental or variable costs of producing an additional or extra unit.
- **Mixed costs.** Costs that fluctuate with volume but not in direct proportion to production or sales. Mixed costs (semivariable or semifixed costs) have elements of both fixed and variable costs (e.g., supervision and inspection). A salesperson's compensation is an example of mixed costs since salary is fixed and commissions are variable.
- **Period costs.** Costs that can be associated with the passage of time, not the production of goods. Period costs are always expensed to the same period in which they are incurred, not to a particular product. Period costs are not identifiable with a product and are not inventoried. Only product costs are included in manufacturing overhead. Period costs are those costs deducted as expenses during the current period without having been previously classified as costs of inventory.
- **Prime costs.** A combination of direct labor and direct material costs. Overhead is not a part of prime costs. The term "prime costs" refers to a unit of finished product. The costs can be identified with and physically traceable to a cost objective.
- **Product costs.** Costs that can be associated with production of certain goods or services. Product costs are those that are properly assigned to inventory when incurred. Inventoriable costs are those costs incurred to produce the inventory and that stay with the inventory as an asset until they are sold. Product costs are expensed (as COGS) in the period the product is sold.

  Examples include property taxes on a factory in a manufacturing company, direct materials, direct labor, and factory overhead. Product costs include direct labor, direct material, and plant manufacturing overhead.
- **Short-run costs.** Costs that vary as output varies for a short period or for a given production capacity.
- **Standard costs.** Predetermined or engineered costs that should be attained under normal conditions of operations. They represent what costs should be.
- **Step costs.** Costs that are constant over small ranges of volume (output) but increase in discrete steps as volume increases. A supervisor of the second shift is an example of step cost. If the step is narrow, it is equal to the variable cost and fixed cost of a wider step.
- **Sunk costs.** Past cost outlays that have already been incurred (e.g., installed factory machinery and equipment cost that becomes a historical cost) or committed to be incurred. Sunk

costs are not relevant to most future costs and current decisions since they cannot be changed by any decision made now or in the future. These costs are irreversible and cannot be affected by choices already made.

APPLICATION OF A SUNK COST CONCEPT

A company has an old machine with a book value of $75,000, with no salvage value, and an estimated remaining life of 12 years. A new machine is available at a cost of $190,000. It has the same estimated remaining life and the same capacity as the old machine, but it would reduce operating costs by $17,000 per year. Which of the following amounts is a sunk cost in the decision whether to replace the old machine?

a. $0
b. $17,000
c. $75,000
d. $190,000

Choice **(c)** is the correct answer. The old machine's book value of $75,000 is an outlay made in the past that cannot be changed. Choice (a) is incorrect. The salvage value does not dictate sunk costs. Choice (b) is incorrect. The $17,000 is a future cost that can be avoided. Choice (d) is incorrect. The $190,000 is a future cost that can be avoided.

- **Unexpired costs.** Portions of cost that remain as assets and continue to generate future benefits.
- **Variable costs.** Costs that fluctuate in total but remain constant per unit as the volume of production or sales changes. For example a variable cost is constant per unit produced but varies in total in direct proportion to changes in production. The cost of fabricator wages should be considered variable because they change in total in direct proportion to the number of similar cables fabricated. General and administrative and other indirect costs can be either fixed or variable. In general, variable costs vary directly with volume or activity. For example, if indirect materials vary directly with volume, then indirect materials can be classified as variable costs.
- **Avoidable costs.** Costs that will not be incurred or costs that may be saved if an ongoing activity is discontinued, changed, or deleted, as in a make-or-buy decision. These costs are relevant costs.
- **Unavoidable costs.** The opposite of avoidable costs. These are costs that are irrelevant; they are sunk costs.
- **Controllable costs.** Costs that can be definitely influenced by a given manager within a given time span. An example includes office supplies purchased by an office manager. In the long run, all costs are controllable. In the short run, costs also are controllable, but they are controlled at different management levels. The higher the management level, the greater the possibility of control.
- **Noncontrollable costs.** Opposite of the controllable costs. These are costs that are unaffected by a manager's decision (e.g., plant rent expense by a plant foreman).
- **Out-of-pocket costs.** Costs that require the consumption of current economic resources (e.g., taxes, insurance). They are the current or near-future expenditures that will require cash outlays to execute a decision.

- **Embodied costs.** Measure sacrifices in terms of their origins, reflecting what was originally given up to acquire and convert the object being costed.
- **Displaced costs.** Measure sacrifices in terms of their ultimate effects on the group making the sacrifice, reflecting the opportunity lost by, or the adverse consequences resulting from, the sacrifice in question. Displaced costs are also called opportunity costs.
- **Discretionary costs.** Costs that arise from periodic budgeting decisions and that have no strong input/output relationship.
- **Opportunity costs.** The maximum net benefit that is forgone by the choice of one course of action over another course of action. They are the economic sacrifice attributable to a given decision. They are the loss associated with choosing the alternative that does not maximize the benefit.
- **Incremental costs.** The increase in total sacrifice identifiable with the specific object, or group of objects, being costed, recognizing that fixed and otherwise joint sacrifices may be increased little, if at all, because of what was done to or for the specific object being costed. Incremental costs also are called differential costs.
- **Differential costs.** The difference in total costs between alternatives.

APPLICATION OF A DIFFERENTIAL COST CONCEPT

ABC Company receives a onetime special order for 5,000 units of Kleen. Variable costs per unit are as follows: direct materials $1.50, direct labor $2.50, variable overhead $0.80, and variable selling $2.00. Fixed costs per year include fixed overhead of $100,000 and fixed selling and administrative cost of $50,000. Acceptance of this special order will not affect the regular sales of 80,000 units. Variable selling costs for each of these 5,000 units will be $1.00.

Question: What is the differential cost to the company of accepting this special order?

Answer: The differential cost is $29,000, as shown below.

We need to consider all differential or incremental costs that would change as a result of the changes in production operations. It should include all variable manufacturing costs and variable selling costs. That is, $1.50 (materials) + $2.50 (direct labor) + $0.80 (variable overhead) + $1.00 (new variable selling cost for 5,000 units) = $5.80. This is multiplied by 5,000 units and gives $29,000. Here fixed costs and variable selling costs for sales of 80,000 units are not relevant.

- **Replacement costs.** Costs that would have to be incurred to replace an asset.
- **Implicit costs.** Imputed costs. They are used in the analysis of opportunity costs.
- **Imputed costs.** Costs that can be associated with an economic event when no exchange transaction has occurred (e.g., the rent for a building when a company "rents to itself" a building).
- **Committed costs.** Two types of committed costs exist: manageable and unmanageable. Manageable committed costs are sacrifices influenced to an important degree by managers' decisions and actions, but these influences have already had most of their effect, setting in motion the chain of events that largely determine the sacrifice in question. Most fixed costs are committed costs. Unmanageable committed costs are sacrifices largely influenced by factors or forces outside managers' control and already set in motion to such an extent that influences have had most of their effect.

- **Uncommitted costs.** Two types of uncommitted costs exist: manageable and unmanageable. Manageable uncommitted costs are sacrifices influenced to an important degree by managers' decisions and actions with plenty of time for these influences to have their effect. Unmanageable uncommitted costs are sacrifices largely influenced by factors or forces outside managers' control with plenty of time for these influences to have their effect.
- **Rework costs.** Costs incurred to turn an unacceptable product into an acceptable product and sell it as a normal finished good.
- **Engineered costs.** Costs resulting from a measured relationship between inputs and outputs.

(v) Cost Behavior

Costs have a behavior pattern. For example, costs vary with volumes of production, sales, or service levels; with the application of the amount of resources; and with the time frame used. Knowing cost-behavior information helps in developing budgets, interpreting variances from standards, and making critical decisions. The manager who can predict costs and their behavior is a step ahead in planning, budgeting, controlling, product pricing, and nonroutine decisions (i.e., make or buy, keep or drop) and in separating cost into its components (i.e., fixed, variable, and mixed costs). In order to make more accurate cost predictions, managers must have superior cost estimates at their disposal.

COST ESTIMATION VERSUS COST PREDICTION

- In cost estimation, an equation is formulated to measure and describe past cost relationships.
- In cost prediction, future costs are forecasted using the cost estimation equation. Here the behavior of past costs will help in predicting future costs.

Two assumptions are made in the estimation of cost functions: (1) cost behavior is a linear function within the relevant range, and (2) variations in the total cost level can be explained by variations in a single cost driver. A cost driver is any factor whose change causes a change in the total cost of a related cost object. Machine hours and direct labor hours are examples of cost drivers in a manufacturing firm.

A cost function is an equation showing the cost-behavior pattern for all changes in the level of the cost driver. A linear cost function is described next.

$$y = a + bx$$

where y = Estimated value
a = Constant or intercept (does not vary with changes in the level of the cost driver within a relevant range)
b = Slope coefficient (the amount of change in total cost [y] for each unit change in the cost driver [x] within the relevant range)

The intercept includes fixed costs that cannot be avoided even at shutdown of the operations. The relevant range is the range of the cost driver in which a valid relationship exists between total cost and the level of the cost driver.

Three types of linear cost functions exist:

1. Variable cost function, where its total cost changes in direct proportion to changes in x within the relevant range because the intercept, a, is zero.
2. Fixed cost function, where the total cost will be constant regardless of the changes in the level of the cost driver.
3. Mixed cost function, also known as semivariable cost, which has both fixed and variable elements. The total costs in the mixed cost function change as the number of units of the cost driver changes, not proportionately.

TECHNIQUES TO SEPARATE COSTS

- Statistics (regression analysis, scatter graphs, and least squares methods)
- High-low method
- Spreadsheet analysis
- Sensitivity analysis
- Managerial judgment

(A) Assumptions Underlying Cost Classifications The classification of costs into their variable cost or fixed cost components is based on three assumptions.

1. The cost object must be specified since costs are variable or fixed with respect to a chosen cost object. Cost objects can be product based or activity based.
2. The time span must be specified. Costs are affected by the time span. The longer the time span, the higher the proportion of total costs that are variable and the lower the fixed costs. Costs that are fixed in the short run may be variable in the long run. There should be a cause-and-effect relationship between the cost driver and the resulting costs. A cost driver may be either an input (e.g., direct labor hour or machine hour) or an output (finished goods). For example, fixed manufacturing costs decline as a proportion of total manufacturing costs as the time span is lengthened from the short run to the medium run to the long run.
3. The relevant range for changes in the cost driver must be specified. Each of the cost-behavior patterns, such as variable cost, fixed cost, or mixed cost, has a relevant range within which the specified cost relationship will be valid. Constraints such as labor agreements and plant capacity levels set the relevant range. If volume exceeds the relevant range, total fixed costs would increase if a new plant is built, and unit variable costs would increase if overtime must be paid.

(B) Cost Estimation Approaches There are four approaches to estimate costs:

1. Industrial engineering method
2. Conference method
3. Account analysis method
4. Quantitative analysis method of current or past cost relationships

(See Exhibit 7.51.) The first three approaches require less historical data than do most quantitative analyses. Therefore, cost estimations for a new product will begin with one or more of the first three methods. Quantitative analysis may be adopted later, after experience is gained. These cost estimation approaches, which are not mutually exclusive, differ in the cost of conducting the analysis, the assumptions they make, and the evidence they yield about the accuracy of the estimated cost function.

1. Industrial engineering method (analyzes relationships between inputs and outputs in physical terms)
2. Conference method (incorporates analysis and opinions gathered from various departments of the firm)
3. Account analysis method (classifies cost accounts in the ledger as variable, fixed, or mixed costs)
4. Quantitive analysis method (uses time-series data based on past cost relationships, regression analysis)

EXHIBIT 7.51 Four Approaches of Cost Estimation

The **industrial engineering method** analyzes the relationship between inputs and outputs in physical terms. Using time and motion studies, physical measures are transformed into standard or budgeted costs. The drawbacks of this method are that it can be time consuming and costly. This method is most often used for significant costs, such as direct labor and direct material costs that are relatively easy to trace to the products. This method is used less often or not used for indirect cost categories, such as manufacturing overhead due to difficulty in specifying physical relationships between inputs and outputs.

The **conference method** develops cost estimates based on analysis and opinions gathered from various departments of an organization. Product costs are developed on consensus of the relevant departments. The advantages of this method include the speed at which cost estimates can be developed, the pooling of knowledge from experts in the functional area, and the resulting credibility of the cost estimates. The disadvantage of this method is that the accuracy of the cost estimates depends on the care taken and attention to detail by those people providing the inputs.

The **account analysis method**, which is widely used, classifies cost accounts in the ledger as variable, fixed, or mixed costs. The method can be thought of as a first step in cost classification and estimation. The conference method is used as a supplement to the account analysis method, which improves the credibility of the latter.

Quantitative analysis methods, such as time-series data or cross-sectional data based on past cost relationships, are often used to estimate cost functions. Time-series data pertain to the same entity over a sequence of past time periods, while cross-sectional data pertain to different entities for the same time period.

STEPS IN ESTIMATING COST FUNCTION

The six steps in estimating the cost function based on an analysis of current or past cost relationships are listed next.

1. Choose the dependent variable (the variable to be predicted). The choice is guided by the purpose for estimating a cost function.

2. Choose the cost driver that is economically plausible (logical and common sense) and accurately measurable. There should be a cause-and-effect relationship between the cost driver and the resulting costs. For example, number of employees is a cost driver for measuring health benefit costs.
3. Collect data on the dependent variable and on the cost driver. The time period (e.g., daily, weekly) used to measure the dependent variable and the cost driver should be identical.
4. Plot the data. The general relationship between the dependent variable and the cost driver (i.e., correlation) can be observed in a plot of the data. A plot of data will reveal whether the cost relation is linear or whether there are outliers. Extreme observations, or outliers, can occur due to errors in recording the data or from an unusual event, such as a labor strike, fire, or flood.
5. Estimate the cost function by using either regression analysis or the high-low method.
6. Evaluate the estimated cost function. The relationship between the dependent variable and the cost driver should be economically plausible. The closer the actual cost observations are to the values predicted by a cost function, the better the goodness of fit of the cost function. In other words, the cost function should be economically plausible and fit the data.

Next we review quantitative methods, such as regression analysis and high-low methods used to estimate cost function.

(C) Regression Analysis Regression analysis provides a model for estimating a cost function and probable error for cost estimates. It measures the average amount of change in the dependent variable, Y', that is associated with a unit change in the amount of one or more independent (or explanatory) variables, x. x is also called the cost driver.

$$Y' = a + bx$$

where a = Constant or intercept
b = Slope coefficient

When only one independent variable (e.g., machine hours) is used, the analysis is called simple regression; when more than one independent variable is used (e.g., machine hours and direct labor hours), it is called multiple regression.

Regression analysis offers a structured approach, based on past data relationships, for identifying cost drivers. All independent variables in a regression model should satisfy these four selection criteria for qualifying as a cost driver:

1. **Economic plausibility.** The relationship between the dependent variable and the independent variable(s) should make economic sense and be intuitive.
2. **Goodness of fit.** The coefficient of determination, r^2, measures the extent to which the independent variable(s) accounts for the variability in the dependent variable. The range of r^2 is from zero to 1, where zero implies no explanatory ability and 1 implies perfect explanatory ability. The goal of maximizing r^2 is called data mining and should not be done at the expense of economic plausibility. A balance is required.
3. **Significance of independent variable(s).** The t-value is computed by dividing the slope coefficient by its standard error. The t-value of a slope coefficient (b) measures the significance of the relationship between changes in the dependent variable and changes in the

independent variable. The coefficient of the chosen independent variable(s) should be significantly different from zero for that independent variable to be considered a possible cost driver.

4. **Specification analysis.** Cost function models make assumptions, such as linearity within the relevant range, constant variance of residuals, independence of residuals, and normality of residuals. When these assumptions are met, the sample values of *a* and *b* from a regression model are the best available linear, unbiased estimates of the population parameters alpha and beta. Testing the assumptions underlying regression analysis is termed specification analysis.

Multicollinearity can exist in a multiple regression when two or more independent variables are highly correlated with each other. This is indicated when a coefficient of correlation (*r*) is greater than 0.70. Multicollinearity has the effect of increasing the standard error of the coefficients of the individual independent variable(s), thus increasing their uncertainty.

Regression analysis and interviews with operating personnel are used to identify cost drivers. For example: The number of products is a cost driver in product design function, the number of suppliers can be a cost driver in a manufacturing operation, and the number of advertisements can be a cost driver in a marketing function.

(D) High–Low Method The high–low method uses two extreme data points (i.e., highest, lowest) to calculate the formula for a line. These two data points could be outliers or may not be representative of all the observations. This method ignores information on all but two observations when estimating the cost function.

Example Application of High–Low Method

	Machine hours	Indirect manufacturing costs
Highest observation of cost driver	5,000	$400,000
Lowest observation of cost driver	2,000	$190,000
Difference	3,000	$210,000

Slope coefficient (*b*) = $210,000/3,000 = $70 per machine hour

Constant (*a*) can be calculated using either highest or lowest observations.

Using the highest observation = $400,000 – $70 (5,000) = $50,000

The high–low estimate of the cost function is $Y' = a + bx$ = $50,000 + $70 (machine hours)

(E) Nonlinearity and Cost Functions A nonlinear cost function is a cost function in which a single constant and a single slope coefficient do not describe in an additive manner the behavior of costs for all changes in the level of the cost driver. For example, even direct materials costs are not always linear variable costs due to quantity discounts. The cost per unit decreases with large orders, but the total costs increase slowly as the cost driver increases.

Step function cost is a situation where the cost of the input is constant over various small ranges of the cost driver, but the cost increases by discrete amounts (in steps) as the cost driver moves from one relevant range to the next. This step-pattern behavior occurs when the input is acquired in discrete quantities but is used in fractional quantities (e.g., vehicle-leasing costs for a package-delivery company).

Batch costs are increased when products are made in batches and a changeover (setup) cost is needed to run a different type of batch. These batch costs are incurred regardless of the size of each batch and have no linear relationship with the number of items in a batch.

(F) Learning Curves and Cost Functions A learning curve is a function that shows how labor hours per unit decline as units of output increase. The learning curve helps managers predict how labor hours or costs will change as more units are produced. The idea behind the learning curve is that workers handling repetitive tasks will become more efficient as they become more familiar with the operation.

Management must be cautious in using the learning curve to establish standards. A steady-state condition can be reached when the effect of the learning curve ceases, and the standard costs would be lower per unit. The corresponding standard cost for the learning curve phase will be higher per unit. If the steady-state standards are imposed during the learning-curve phase, an unfavorable efficiency variance between standards and actual performance may persist, and the employees might reject the standards as unattainable. This situation will lead to low morale and low productivity.

The benefit of the learning curve can be clearly seen with new products, new workers, and new machines. Learning curves are applied more frequently to direct labor and overhead and less frequently to direct materials. In addition to volume as a driver of learning, product design and process configuration are being researched as possible drivers of learning.

APPLICATION OF LEARNING-CURVE PRINCIPLE

Example: Sun Corporation has received an order to supply 240 units of a product. The average direct labor cost was estimated to be $40,000 per unit for the first lot of 30 units. The direct labor is subject to a 90% learning curve.

Question: What is the cumulative average unit cost of labor for production of 240 units?

Answer: The cumulative average unit cost of labor for production of 240 units is $29,160, as shown.

Cumulative number of lots	Cumulative number of units	Cumulative average unit cost of labor
1	30	($40,000 × 1) = $40,000
2	60	($40,000 × .9) = 36,000
4	120	($36,000 × .9) = 32,400
8	240	($32,400 × .9) = 29,160

The term **experience curve** describes the broader application of the learning curve to include not only manufacturing cost but also marketing, distribution, and customer service areas. An experience curve is a function that shows how full costs per unit decline as units of output increase.

(G) Learning-Curve Models Two learning-curve models exist: the cumulative average-time learning model and the incremental unit-time learning model.

In the **cumulative average-time learning model**, the cumulative average time per unit is reduced by a constant percentage each time the cumulative quantity of units produced is doubled. Learning occurs at a faster rate with this method as compared to the incremental unit-time model.

In the **incremental unit-time learning model**, the time needed to produce the last unit is reduced by a constant percentage each time the cumulative quantity of units produced is doubled. This method requires a higher cumulative total time to produce two or more units as compared with cumulative average-time model.

The deciding factor between the cumulative average-time and incremental unit-time learning model is the ability to approximate the behavior of labor-hour usage as output levels increase.

(d) Relevant Costs

(i) Differential Analysis

Managers must consider the effects of alternative decisions on their businesses. We discuss differential analysis, which reports the effects of alternative decisions on total revenues and costs. Planning for future operations involves decision making. For some decisions, revenue and cost data from the accounting records may be useful. However, often the revenue and cost data for use in evaluating courses of future operations or choosing among competing alternatives are not available in the accounting records and must be estimated. These estimates include relevant revenues and costs. The relevant revenues and costs focus on the differences between each alternative. Costs that have been incurred in the past are not relevant to the decision. These costs are called **sunk costs**.

FOCUS OF RELEVANT COSTS

The relevant revenues and costs focus on the difference between each alternative.

Differential revenue is the amount of increase or decrease in revenue expected from a course of action as compared with an alternative. To illustrate, assume that certain equipment is being used to manufacture calculators, which are expected to generate revenue of $150,000. If the equipment could be used to make digital clocks, which would generate revenue of $175,000, the differential revenue from making and selling digital clocks is $25,000.

Differential cost is the amount of increase or decrease in cost that is expected from a course of action as compared with an alternative. For example, if an increase in advertising expenditures from $100,000 to $150,000 is being considered, the differential cost of the action is $50,000.

Differential income or loss is the difference between the differential revenue and the differential costs. Differential income indicates that a particular decision is expected to be profitable, while a differential loss indicates the opposite.

Differential analysis focuses on the effect of alternative courses of action on the relevant revenues and costs. For example, if a manager must decide between two alternatives, differential analysis would involve comparing the differential revenues of the two alternatives with the differential costs.

Differential analysis can be used in analyzing these alternatives:

- Leasing or selling equipment
- Discontinuing an unprofitable segment
- Manufacturing or purchasing a needed part (make-or-buy analysis)
- Replacing usable fixed assets
- Processing further or selling an intermediate product
- Accepting additional business at a special price

(ii) Application of Relevant Cost Concept

When deciding whether to accept a special order from a customer, the best thing to do is to compare the total revenue to be derived from this order with the total relevant costs incurred for this order. The key terms are incremental relevant costs and incremental relevant revenues. The relevant costs are those that vary with the decision.

Long-term fixed costs should be excluded from the analysis since they will be incurred regardless of whether the order is accepted. Direct labor, direct materials, variable manufacturing overhead, and variable selling and administrative costs are relevant because they will not be incurred if the special order is not accepted. Incremental fixed costs would be relevant in short-term decision making under certain situations.

(e) Cost-Volume-Profit Analysis

Cost-volume-profit (CVP) analysis helps managers who are making decisions about short-term duration and for specific cases where revenue and cost behaviors are linear and where volume is assumed to be the only cost and revenue driver. CVP is an approximation and low-cost tool.

KEY CONCEPTS TO REMEMBER: What Are Cost or Revenue Drivers?

- A cost driver is any factor whose change causes a change in the total cost of a related cost object.
- A revenue driver is any factor whose change causes a change in the total revenue of a related product or service.
- There are many cost drivers and revenue drivers besides volume of units produced or sold. Examples affecting total cost and revenue include changes in quantity of materials and changes in setting prices, respectively.

CVP analysis is a straightforward, simple-to-apply, widely used management tool. It answers questions such as: How will costs and revenues be affected if sales units are up or down by X%? If price is decreased or increased by X% percent? A decision model can be built using CVP relationships for choosing among courses of action. *CVP analysis tells management what will happen to financial results if a specific level of production or sales volume fluctuates or if costs change.*

An example of a decision model is the break even point (BEP), which shows the interrelationships of changes in costs, volume, and profits. It is the point of volume where total revenues and total costs are equal. No profit is gained or loss incurred at the BEP.

(i) Methods for Calculating Breakeven Point

Three methods available for calculating the BEP are shown in Exhibit 7.52.

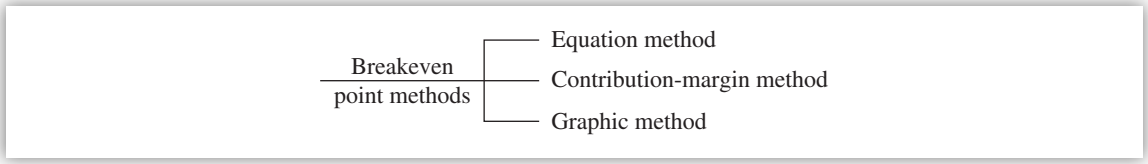


EXHIBIT 7.52 Breakeven Point Methods

An increase in the BEP is a red flag for management to analyze all its CVP relationships more closely.

(A) Equation Method The equation method is general and thus is easier to apply with multiple products, multiple costs and revenue drivers, and changes in the cost structure. At BEP, the operating income is zero.

Formula

(Unit sales price × Number of units) − (Unit variable cost × Number of units) − Fixed costs = Operating income or Sales − Variable costs − Fixed costs = Operating income

Example

Price is $100, variable cost is $60, fixed costs are $2,000. What are the breakeven units?

$$100N - 60N - 2{,}000 = 0$$
$$40N = 2{,}000$$
$$N = 2{,}000/40 = 50 \text{ units}$$

(B) Contribution Margin Method CM is equal to sales minus all variable costs. BEP is calculated as follows:

$$\text{BEP} = \text{Fixed costs}/\text{Unit CM}$$

Using the same example, BEP = 2,000/(100 − 60) = 2,000/40 = 50 units

A desired target operating income can be added to the fixed costs to give a new BEP that tells how many units must be sold to generate enough CM to cover total fixed costs plus target operating income.

The BEP tells how many units of product must be sold to generate enough CM to cover total fixed costs. The CM method is valid only for a single product and a single cost driver. The method is a restatement of the equation method in a different form. Either method can be used to calculate the BEP.

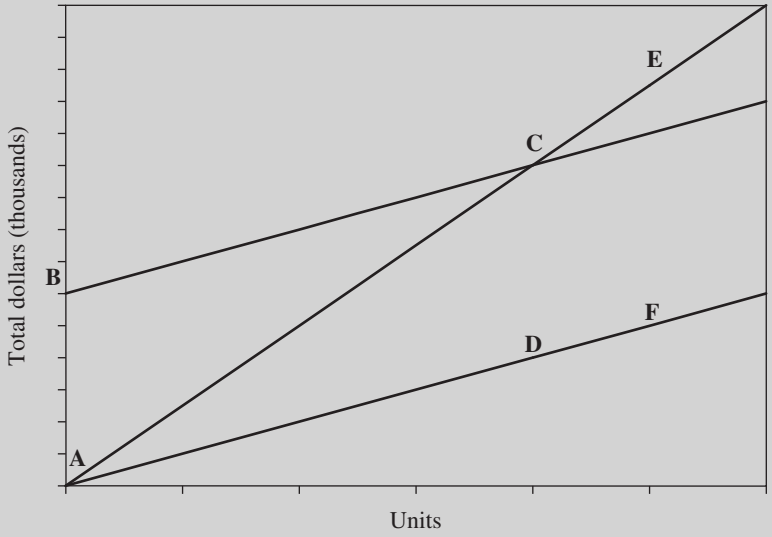
(C) Graphic Method A CVP chart results when units are plotted on the x-axis and dollars on the y-axis. The BEP is where the total sales line and total cost line intersect. The total sales line begins at the origin because if volume is zero, sales revenue will be zero too.

Examples: Volume versus Costs versus Sales

- As volume increases, total fixed costs remain the same over the entire volume range.
- As volume increases, both total variable costs and sales increase.

The total fixed cost line will be flat because fixed costs are constant across a wide range of volumes. Linear CVP analysis is approximate under perfect competition, thus showing the link between cost accounting and economics. In economics, the slope of the total revenue (TR) function equals marginal revenue (MR), which equals sales per unit. The slope of the total cost (TC) function is marginal cost (MC), which equals variable cost per unit. The sales price per unit and variable cost per unit are constant across a wide range of volumes only if there is perfect competition in input and output markets. However, this is not true for imperfect competition, where sales price must be reduced to increase volume.

Use the following CVP chart for Examples 1 and 2.



Example 1

Which of the following labeled points on this chart is the BEP?

a. Point A
b. Point B
c. Point C
d. Point D

Choice **(c)** is the correct answer. Point C is the intersection of the total cost line and the total revenue line, which is the BEP. Choice (a) is incorrect. Point A is the origin, where total revenues are zero and there is a loss equal to the amount of fixed costs. Choice (b) is incorrect. Point B is the total cost line at zero activity, which is the amount of total fixed costs. Choice (d) is incorrect. Point D is on the total variable cost curve and represents the total variable costs at the BEP.

Example 2

Which of the following items is graphically represented on the CVP chart as the difference between labeled points E and F?

a. Total profit
b. Total variable costs
c. Total fixed costs
d. Total CM

Choice **(d)** is the correct answer. The difference between labeled points E (which is on the total revenue line) and point F (which is on the total variable cost line) is total CM. Choice (a) is incorrect because it is on point C. Choice (b) is incorrect because it is on point D. Choice (c) is incorrect because it is on point B. Choices (a), (b), and (c) are not between points E and F.

(ii) CVP Assumptions and Their Limitations

(A) Assumptions We already learned that the CVP relationships hold true for only a limited range of production or sales volume levels. This means that these relationships would not hold if volume fell below or rose above a certain level. A list of assumptions is presented next.

- The behavior of total revenues and total costs is linear over the relevant range of volume.
- Selling prices, total fixed costs, efficiency, and productivity are constant.
- All costs can be divided neatly into fixed and variable components. Variable cost per unit remains constant.
- A greater sales mix will be maintained as total volume changes.
- Volume is the only driver of costs.
- The production volume equals sales volume, or changes in beginning and ending inventory levels are zero.

(B) Limitations There are many limitations to the CVP assumptions just made. Volume is only one of the factors affecting cost behavior. Other factors include unit prices of inputs, efficiency, changes in production technology, civil wars, employee strikes, laws, and regulations. *Profits are affected by changes in factors besides volume.* A CVP chart must be analyzed in total by considering all assumptions and their limitations.

(iii) Ways to Lower the Breakeven Point

The next strategies should help in lowering the BEP, which means fewer units need to be sold, which, in turn, contributes more to profits. (Note that the strategies are not order ranked).

- Reduce the overall fixed costs.
- Increase the CM per unit of product through an increase in sales prices.
- Increase the CM per unit of product through decreases in unit variable costs.
- Increase the CM per unit through both an increase in sales prices and a decrease in unit variable costs.
- Set a hiring freeze for new employees.
- Limit merit increases for senior executives.
- Cut the annual percentage salary rate increase for all salaried employees.
- Reduce overtime pay for all employees to reduce labor costs.
- Reduce the number of employees on the payroll.

- Improve employee productivity levels.
- Increase machine utilization rates.

(iv) Sensitivity Analysis in CVP

A CVP model developed in a dynamic environment determined that the estimated parameters used may vary between limits. Subsequent testing of the model with respect to all possible values of the estimated parameters is termed a sensitivity analysis.

Sensitivity analysis is a management tool that will answer questions such as: What will operating income be if volume changes from the original prediction? What will operating income be if variable costs per unit decrease or increase by X%? If sales drop, how far can they fall below budget before the BEP is reached? The last question can be answered by the margin of safety tool. The margin of safety is a tool of sensitivity analysis and is the excess of budgeted sales over the breakeven volume.

Sensitivity analysis is a what-if technique aimed at asking how a result will be changed if the original predicted data are not achieved or if an underlying assumption changes. It is a measure of changes in outputs resulting from changes in inputs. It reveals the impact of changes in one or more input variables on the output or results.

(v) Changes in Variable and Fixed Costs

Organizations often face a trade-off between fixed and variable costs. Fixed costs can be substituted for variable costs and vice versa. This is because variable costs and fixed costs are subject to various degrees of control at different volumes—boom or slack. For example, when a firm invests in automated machinery to offset increase in labor rates, its fixed costs increase, but unit variable costs decrease.

(vi) Contribution Margin and Gross Margin

CM is the excess of sales over all variable costs, including variable manufacturing, marketing, and administrative categories. Gross margin, also called gross profit, is the excess of sales over the cost of the goods sold. CM and GM would be different for a manufacturing company. They are equal only when fixed manufacturing costs included in COGS are the same as the variable nonmanufacturing costs, which is a highly unlikely event.

- Variable manufacturing, marketing, and administrative costs are subtracted from sales to get CM but not GM.
- Fixed manufacturing overhead is subtracted from sales to get GM but not CM.
- Both CM and GM can be expressed as totals, as an amount per unit, or as percentages of sales in the form of ratios.

An example of GM and of CM is presented next.

Gross margin		**Contribution margin**	
Sales	$50,000	Sales	$50,000
Manufacturing		Variable manufacturing costs	$20,000
Cost of goods sold	$30,000	Variable nonmanufacturing costs	$ 5,000
Gross margin	$20,000	Total variable costs	$25,000
		Contribution margin	$25,000

Example Application of Contribution Margin Concept

A department store prepares segmented financial statements. During the past year, the income statement for the perfume department located near the front entrance was:

Sales	$200,000
Cost of goods sold	120,000
Gross profit	80,000
Janitorial expense	5,000
Sales commissions	40,000
Heat and lighting	4,000
Depreciation	3,000
Income before taxes	$ 28,000

Janitorial expense, heat and lighting, and depreciation are allocated to the department based on square footage. Sales personnel work for only one department and are paid on commission. What is the perfume department's CM?

a. $28,000
b. $31,000
c. $37,000
d. $40,000

Choice **(d)** is the correct answer. CM is the gross profit of $80,000 minus the $40,000 of sales commissions, that is, $40,000. Choice (a) is incorrect. This is net income, as given. Choice (b) is incorrect. Janitorial and heat and light are fixed costs ($80,000 – $40,000 – $5,000 – $4,000). Choice (c) is incorrect. Depreciation is a fixed cost, hence not a part of CM ($80,000 – $40,000 – $3,000).

(vii) Profit-Volume Chart

The profit-volume chart is preferable to the cost-volume-profit chart because it is simpler to understand. The profit-volume chart shows a quick, condensed comparison of how alternatives on pricing, variable costs, or fixed costs affect operating income as volume changes. The *y*-axis shows he operating income, and the *x*-axis represents volume (units or dollars).

Due to operating leverage, profits increase during high volume because more of the costs are fixed and do not increase with volume. Profits decrease during low volume because fixed costs cannot be avoided despite the lower volume.

(viii) Effect of Sales Mix and Income Taxes

Sales mix is the relative combination of quantities of products that constitute total sales. A change in sales mix will cause actual profits to differ from budgeted profits. It is the combination of low-margin or high-margin products that causes the shift in profits, despite achievement of targeted sales volume.

There will be a different BEP for each different sales mix. A higher proportion of sales in high-CM products will reduce the BEP. A lower proportion of sales in small-CM products will increase the BEP. Shifting marketing efforts to high-CM products can increase the operating income and profits.

Management is interested in the effect of various production and sales strategies on the operating income, not so much on BEP. Both operating income and BEP are dependent on the assumptions made (i.e., if the assumptions change, operating income and BEP will also change).

The impact of income taxes is clear. The general equation method can be changed to allow for the impact of income taxes, as shown next.

$$\text{Target operating income} = (\text{Target net income})/(1 - \text{Tax rate})$$

Each unit beyond the BEP adds to net income at the unit CM multiplied by (1 – Tax rate). However, the BEP itself is unchanged. This is because no income tax is paid at a level of zero income. In other words, an increase in income tax rates will not affect the BEP.

(f) Transfer Pricing

Transfer pricing involves inter- or intracompany transfers, whether domestic or international. A **transfer price** is the price one unit of a corporation charges for a product or service supplied to another unit of the same corporation. The units involved could be either domestic or international, and the products involved could be intermediate products or semifinished goods.

Reasons for establishing transfer pricing in either domestic or international operations are listed next.

- Performance evaluation of decentralized operations
- Overall minimization of taxes to a corporation
- Minimization of custom duties and tariffs
- Minimization of risks associated with movements in foreign currency exchange rates
- Circumventing restrictions on profit remittance to corporate headquarters
- Motivation of unit managers

KEY CONCEPTS TO REMEMBER: Supplying Unit and Receiving Unit

Supplying unit (seller)	Receiving unit (buyer)
Domestic	Domestic
Domestic	International
International	International
International	Domestic

- If the seller is a profit or investment center, transfer pricing is most likely to cause conflicts.
- If the seller is a cost center, it has less (no) incentive to maximize sales revenues. Hence, there is little or no conflict.

(i) Transfer Pricing Methods

Three methods are available for determining transfer prices: market based, cost based, and negotiated (see Exhibit 7.53).

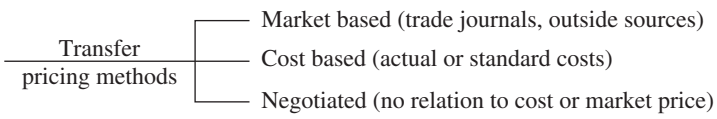


EXHIBIT 7.53 Transfer Pricing Methods

- **Market-based transfer prices.** The price appearing in a trade journal or other independent (outside) sources establishes the transfer price of a product or service. Difficulty in obtaining market price forces corporations to resort to cost-based transfer prices. This method is widespread in use.

TRANSFER PRICES ALERT

There is no single best method in determining transfer prices. Ideally, the chosen method should help the unit manager to make optimal decisions for the organization as a whole.

- **Cost-based transfer prices.** The costs used could be either actual costs or standard costs and include variable manufacturing costs, or absorption (full) costs. Use of full cost-based prices leads to suboptimal decisions in the short run for the company as a whole. This method is also widespread in use. Standard costs are used more widely than actual costs to motivate the seller to produce efficiently. If transfer prices are based on actual costs, sellers can pass along costs of inefficiency to buyers.
- **Negotiated transfer prices.** These are the negotiated prices between units of a corporation and may not have any relation to either cost or market-price data. Unit autonomy is preserved. Drawbacks include time-consuming and drawn-out negotiations, which may not lead to goal congruence. Weak bargaining units may lose out to strong ones.

The choice of a transfer pricing method affects the operating income of individual units. Next, we will discuss how the criteria of goal congruence, managerial effort, and unit autonomy affect the choice of transfer-pricing methods.

(ii) Transfer Pricing Management

Goal congruence exists when individual goals, group goals, and senior management goals coincide. Under these conditions, each unit manager acts in his or her own best interest, and the resulting decision is in the long-term best interest of the company as a whole. A transfer price method should lead to goal congruence.

A sustained high level of **managerial effort** can lead to achievement of goals. A transfer price method promotes management effort if sellers are motivated to hold down costs and buyers are motivated to use the purchased inputs efficiently.

Senior management should allow a high level of **unit autonomy** in decision making in a decentralized organization. This means that a transfer price method should preserve autonomy if unit managers are free to make their own decisions and are not forced to buy or sell products at a price that is unacceptable to them.

KEY CONCEPTS TO REMEMBER: Transfer Pricing

- If no incremental fixed costs are incurred, variable costs are a floor transfer price since the seller will not sell for less than the incremental costs incurred to make the product.
- Market price is a ceiling transfer price since the buyer will not pay more than market price.
- Therefore, the final transfer price usually falls between variable cost and market price.
- Corporations may use different transfer price methods for different items (i.e., market-based pricing for big-ticket items, variable cost-plus for low-value items, and negotiated prices for midrange items).

(iii) Dual Pricing

Dual pricing uses two separate transfer pricing methods to price each inter-unit transaction. It uses the two methods because a single transfer price seldom meets the criteria of goal congruence, managerial effort, and unit autonomy. An example of dual pricing is when the selling unit receives a full-cost plus markup-based price and the buying unit pays the market price for the internally transferred products.

The dual pricing method reduces the goal-congruence problems associated with a pure cost-plus-based transfer pricing method. Some of the drawbacks of dual pricing are listed next.

- The manager of the supplying unit may not have sufficient incentives to control costs.
- It does not provide clear signals to unit managers about the level of decentralization senior managers are seeking.
- It tends to insulate managers from the frictions of the marketplace (i.e., knowledge of units' buying and selling market forces).

(iv) International Transfer Pricing

Because MNCs must deal with transfer pricing and international taxation, knowledge of international laws related to these areas is important. A transfer is a substitute for a market price and is recorded by the seller as revenue and by the buyer as COGS. The transfer pricing system should motivate unit managers not to make undesirable decisions at the expense of the corporation as a whole. The ideal manager would act in the best interests of the company as a whole, even at the expense of the reported profits of his or her own unit. For this to happen, the managers must be rewarded when they choose companywide goal congruence over unit performance.

Example Application of Transfer Pricing Method

Example 1

Unit A sells 500 units of product X to Unit B for $5 per unit. The $5 selling price is the transfer price.

Example 2

Unit A sells 500 units of product X to Unit B for $6 per unit. The normal market price is $4 per unit. Unit A shows increased sales of $2 per unit and a higher profit. Unit B shows the COGS has increased by $2 per unit and therefore has a lower profit. This example clearly violates the goal congruence principle since Unit A charges an inflated transfer price for products transferred to Unit B.

GOAL CONGRUENCE AND DECISION MAKING

- Desirable decisions enhance goal congruence.
- Undesirable decisions stifle goal congruence.
- Undesirable decisions can be minimized when the performance evaluation system is compatible with the transfer system.

According to Mueller and his co-authors,[2] the international transfer pricing system must also attempt to accomplish objectives that are irrelevant in a purely domestic operation. These objectives include:

- Worldwide income tax minimization.
- Minimization of worldwide import duties.
- Avoidance of financial restrictions.
- Managing currency fluctuations.
- Winning host-country government approval.

Each objective is discussed briefly.

Worldwide income tax minimization. The transfer pricing system can be used to shift taxable profits from a country with a higher tax rate to a country with a lower tax rate; the result is that the MNC retains more profit after taxes. For example, the Cayman Islands have long been considered a tax haven for MNCs due to the zero corporate income tax rate. Pakistan has the highest corporate income tax rate: 50%.

Minimization of worldwide import duties. Transfer prices can reduce tariffs. Import duties are normally applied to intracompany transfers as well as sales to unaffiliated buyers. If the goods are transferred in at low prices, the resulting tariffs will be lower.

Tariffs interact with income taxes. Two associations exist: (1) low import duties and high income tax rates, and (2) high import duties and low income tax rates. There is a trade-off between income taxes and tariffs. The MNC has to evaluate the benefits of a lower (higher) income tax in the importing country against a higher (lower) import tariff as well as the potentially higher (lower) income tax paid by the MNC in the exporting country.

Avoidance of financial restrictions. Foreign governments place certain types of economic restrictions on MNC operations with respect to the amount of cash transferred between the countries and the amount of a tax credit or subsidy allowed. A subsidy is a payment from the government to the subsidiary unit and the nondeductibility of certain expenses provided by the parent against taxable income. This includes R&D expenses, general and administrative expenses, and royalty fees.

Some ways to avoid these financial restrictions include setting a high transfer price on goods imported into the country, which would facilitate the desired movement of cash because the importing subsidiary must remit payment; charging a high transfer price on exported products, which will be followed by a larger tax credit or higher subsidy; or inflating the transfer price of imports to the subsidiary so that the nondeductibility of certain expenses can be recovered.

[2] G. Mueller, H. Gernon, and G. K. Meek, *Accounting: An International Perspective*, (Burr Ridge, IL: Irwin), 1994.

Two options are available to an MNC to avoid financial restrictions:

- If the goal is to show lower profitability, high transfer prices on imports to subsidiaries can be used. This objective is appropriate to discourage potential competitors from entering the market or takeover by outsiders.
- If the goal is to show higher profitability, lower transfer prices on imports to subsidiaries can be used. Higher profits may trigger the subsidiary's employees to demand higher wages or profit-sharing plans or takeover by outsiders. Lower transfer prices on imports could improve the subsidiary's financial position, which facilitates local financing and enjoys a competitive edge during its initial stages of growth.

Managing currency fluctuations. A country suffering from balance-of-payments problems may decide to devalue its national currency. Losses from such devaluations may be avoided by using inflated transfer prices to transfer funds from the country to the parent or to some other affiliate unit.

Balance-of-payments problems often result from an inflationary environment. Inflation erodes the purchasing power of the MNC's monetary assets. Using inflated transfer prices on goods imported to such an environment may offer a timely cash removal method.

Winning host-country government approval. Maintaining positive relations with the host government is a good idea since the government is concerned about both intercorporate pricing and its effect on reported profits and continually changing and manipulating transfer prices. For example, using unfavorable transfer prices to a country's economic detriment could result in the loss of goodwill. It is a trade-off between sacrificing some profits and satisfying foreign government authorities. Factors such as tax rates, tariffs, inflation, foreign exchange controls, government price controls, and government stability need to be considered when analyzing the trade-offs.

(v) Transfer Pricing Choices

Basically, two choices exist in transfer pricing: market-based pricing and cost-based pricing. The benefits of using market-based pricing are listed next.

- Divisional profitability approaches the real economic contribution of the subsidiary to the total MNC.
- Such pricing creates a sense of competition among various subsidiaries.
- It facilitates better evaluation of a subsidiary's performance
- Market-based pricing incurs less scrutiny from foreign government tax authorities

Pitfalls of using market-based pricing are listed next.

- Subsidiaries need not be autonomous profit centers.
- Subsidiary managers may not have the authority to make autonomous decisions.
- There may not be an intermediate market in order to establish a free competitive market price
- The MNC may not have much flexibility to manipulate profits and cash flows.

If market prices are either unavailable or cannot be reasonably estimated, then cost-based transfer prices are conveniently determined because the information on costs is available. Cost may be

the full cost, a variable cost, or marginal cost with a markup added to allow the selling subsidiary some percentage of profit.

Disadvantages of cost-based transfer pricing are listed next.

- The selling party has no incentive to control costs or to operate efficiently.
- Since inefficiencies can be passed along to the purchasing subsidiary, undesirable behavior may result in the form of poor decision making.

KEY CONCEPTS TO REMEMBER: Transfer Pricing Choices

- A highly decentralized MNC would be expected to use market-based transfer prices. Smaller firms favor decentralized operations to achieve their objectives and to avoid foreign government scrutiny.
- A centralized MNC would control the setting of cost-based transfer prices. Large firms are generally more centralized due to worldwide optimization of objectives. Cost-based transfer pricing provides flexibility and control.
- The nationality of the parent company's management also affects whether the MNC uses market prices or costs in establishing a transfer price.

(vi) Taxes and Transfer Pricing

Intercompany transactions from an MNC point of view are subject to Section 482 of the Internal Revenue Code of the United States. Section 482 gives the Internal Revenue Service (IRS) the authority to reallocate income and deductions among subsidiaries if it determines that this is necessary to prevent tax evasion (the illegal reduction of taxes). The key test is whether intercompany sales of goods or services appear to be priced at arm's-length market values. Among items the IRS will scrutinize are trademarks, patents, R&D cost, and management services.

The IRS allows three pricing methods considered arm's length: (1) the comparable uncontrolled price method (i.e., market-based transfer pricing), (2) the resale price method (i.e., sales price less markup), and (3) the cost-plus method (i.e., cost-based transfer pricing).

TAX OBJECTIVES IN CONFLICT: IRS VERSUS MNC

- The IRS's objective is to determine the MNC's tax liability.
- The MNC's objective is after-tax profit maximization.
- These two objectives conflict.
- It is possible that a U.S. MNC may use one transfer price for internal financial reporting and another for computing its U.S. tax liability.

(g) Responsibility Accounting

(i) Overview

Managers are responsible and accountable for their decisions and actions in planning and controlling the resources of the organization. Resources include physical, human, and financial ones. Resources are used to achieve the organization's goals and objectives. Budgets help to quantify the resources required to achieve goals.

The concept of responsibility accounting emerged because a few senior managers at the top cannot run all parts of a business effectively. To improve performance, the organization is divided into centers, product lines, divisions, and units so that a lower-level manager is responsible for a specific center, product line, division, or unit.

(ii) Definition of Responsibility Accounting

Each manager is in charge of a responsibility center and is accountable for a specified set of activities and operations within a segment of the organization. The degree of responsibility varies directly with the manager's level. Responsibility accounting is a system that measures the plans and actions of each responsibility center. Four types of responsibility centers are common, as shown in Exhibit 7.54.

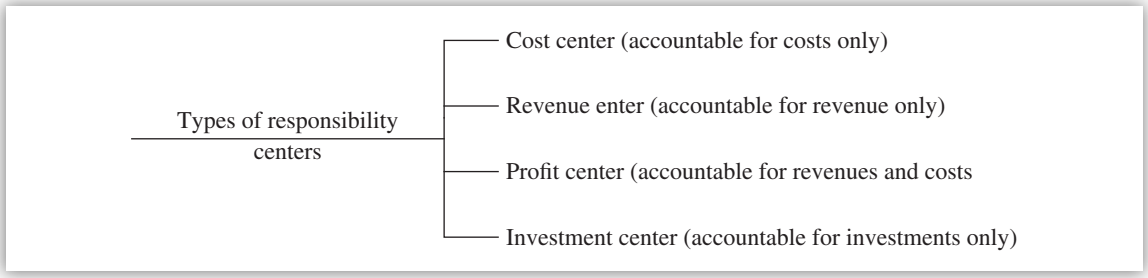


EXHIBIT 7.54 Types of Responsibility Centers

In a **cost center**, a manager is accountable for costs only (e.g., a manufacturing plant). In a **revenue center**, a manager is accountable for revenues only (e.g., a product manager or brand manager). In a **profit center**, a manager is accountable for revenues and costs (e.g., a division). In an **investment center**, a manager is accountable for investment (e.g., a division revenues and costs).

A major **advantage** of the responsibility accounting approach is that costs can be traced to either the individual who has the best knowledge about the reasons for cost increase or the activity that caused the cost increase. A major **disadvantage** is the behavioral implications of the approach on managers whose performance is to be evaluated.

Managers should be held accountable for the costs that they have control over. Controllability is the degree of influence that a specific manager has over costs, revenues, and investment. A controllable cost is any cost that is subject to the influence of a given manager of a given responsibility center for a given time span. Controllable costs should be separated from uncontrollable costs in a manager's performance report.

KEY CONCEPTS TO REMEMBER: Responsibility Accounting

- Most managers have partial control over their costs; their rewards depend on factors they cannot control.
- Managers should be compensated according to risk taking regardless of who controls the costs. Otherwise, management turnover, frustration, and low motivation will set in.
- Managers should be able to influence activities even they he do not have full control over costs.
- A manager's behavior can be changed by senior management by switching from cost center to profit center if it helps the organization.

In responsibility accounting, feedback is crucial. When budgets are compared with actual results, variances occur. The key is to use variance information to raise questions and seek answers from the right party. Variance information should not be abused—in other words, it should not be used to lay blame on others. *Variances invoke questions as to why and how, not who.*

(h) Operating Budgets

A budgeting system includes both expected results and historical or actual results. Such a system builds on historical, or actual, results and expands to include consideration of future, or expected, results. A budgeting system guides managers into the future.

Budget system → Forward looking

Historical cost system → Backward looking

A budget is a quantitative expression of a plan of action. It will aid in the coordination of various activities or functions throughout the organization. The master budget by definition summarizes the objectives of all subunits of an organization (i.e., both operating budgets and financial budgets). The master budget helps in coordinating activities, implementing plans, authorizing actions, and evaluating performance (see Exhibit 7.55).

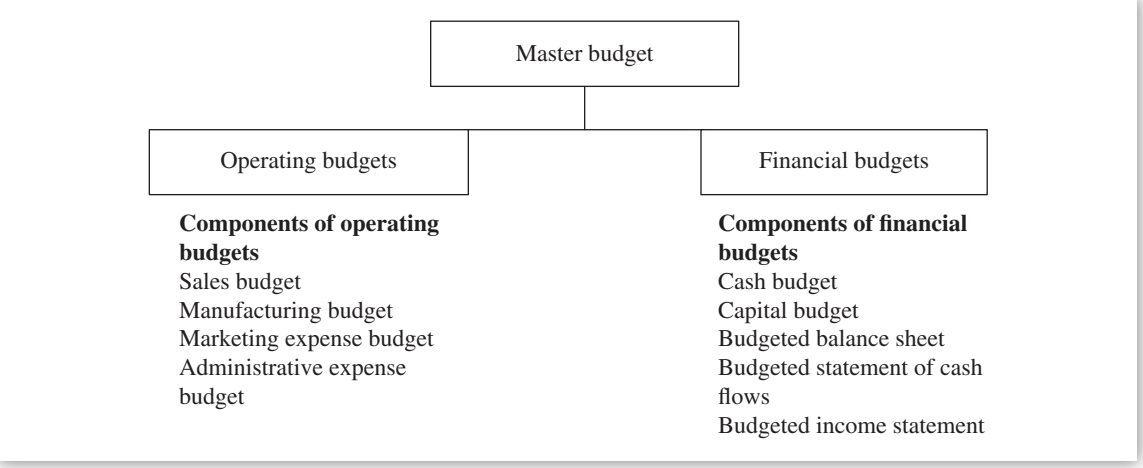


EXHIBIT 7.55 Master Budget and Its Components

The master budget captures the financial impact of all the firm's other budgets and plans. Although the master budget itself is not a strategic plan, it helps managers to implement the strategic plans. The master budget focuses on both operating decisions and financing decisions. Operating decisions concentrate on the acquisition and use of scarce resources.

Financing decisions center on how to get the funds to acquire resources. It focuses on operating decisions and budgets.

(i) Benefits of Operating Budgets

Benefits to be derived from budgets are listed next.

- Budgets are planning tools. Budgets force managers to look into the future and make them prepare to meet uncertainties and changing business conditions.

- Budgets provide a starting point for discussing business strategies. In turn, these strategies direct long-term and short-term planning. Therefore, strategic plans and budgets are interrelated and affect one another.

BUDGET ALERTS

Be alert to communication breakdowns, empire-building (self-centered) efforts of managers during the budgeting process, and behavioral implications of budgets.

- Budgeted performance is better than historical data for judging or evaluating employee performance. This is because employees know what is expected of their performance. A major drawback of using historical data is that inefficiencies and bad decisions may be buried in past actions.
- Budgets can be valuable vehicles for communication with interested parties. Budgets help coordinate activities of various functions within the organization to achieve overall goals and objectives.
- Budgets are control systems. They help to control waste of resources and search out weaknesses in the organizational structure.
- A budget should be implemented so as to gain acceptance by employees. This requires a buy-in by employees, senior management support, and lower-level management involvement.
- A budget should be set tight but attainable and flexible. A budget should be thought of as a means to an end, not the end in itself.
- A budget should not prevent managers from taking prudent action. Nonetheless, managers should not disregard the budget entirely.

(ii) Different Dimensions in Operating Budgets

The time period for budgets varies from one year to five or more years. The common budget period is one year, broken down by quarters and months. Four types of budgets emerge from the time coverage and update point of view: short-term, long-term, static, and continuous budgets.

1. Short-term budgets (operating budgets) have a time frame of one to two years.
2. Long-term budgets (strategic budgets) have a time frame of three to five or more years.
3. Static budgets are the original budgeted numbers, which are not changed. The time frame does not change.
4. Continuous budgets are also called rolling budgets. A 12-month forecast is always available by adding a month in the future as the month just ended is dropped. The time frame keeps changing in the continuous budgets.

LENGTH AND CHOICE OF THE BUDGET

- The length of the budget period depends on the nature of the business (i.e., stable versus unstable). Stable firms will have longer budget periods than unstable firms.
- The choice of budget periods depends on the objectives, uses, and reliability of the budget data.

Budgets should be viewed positively, not negatively. Although budget preparation is mechanical, its administration and interpretation require patience, education, and people skills. Budgets are a positive device designed to help managers choose and accomplish objectives. However, budgets are not a substitute for bad management or poor accounting system.

(iii) How Operating Budgets Are Prepared

The **master budget** (static budget) is developed after the goals, strategies, and long-range plans of the organization have been determined. It summarizes the goals of the subunits or segments of an organization. This information summarizes, in a financial form, expectations regarding future income, cash flows, financial position, and supporting plans. The functions of budgets include planning, coordinating activities, communicating, evaluating performance, implementing plans, motivating, and authorizing actions. The master budget contains the operating budget.

A detailed budget is prepared for the coming fiscal year along with some less detailed amounts for the following years. Budgets may be developed from the top-down or the bottom-up approach. With the **top-down approach**, upper management determines what it expects from subordinate managers. Subordinate managers may then negotiate with upper management concerning the items they feel are unreasonable. With the **bottom-up approach**, lower-level managers propose what they expect to accomplish and the required resources. Upper management then makes suggestions and revisions. Budgets may be used for long-range planning, but the typical planning-and-control budget period is one year. This annual budget may be broken down into months or quarters and continuously updated.

HOW MANY BUDGETS ARE THERE?

- **Budgeted balance sheet.** This budget reflects the expected balance sheet at the end of the budget period. The budgeted balance sheet is determined by combining the estimate of the balance sheet at the beginning of the budget period with the estimated results of operations for the period obtained from the budgeted income statements and estimating changes in assets and liabilities. These changes in assets and liabilities result from management's decisions regarding capital investment in long-term assets, investment in working capital, and financing decisions.
- **Budgeted income statement or operating budget.** This budget reflects the income expected for the budget period.
- **Budgets for other expenses.** These budgets may be broken down according to expense category, depending on the relative importance of the types of expenses (i.e., selling, administrative, R&D, etc.).
- **Cash budget.** The cash budget summarizes cash receipts and disbursements and indicates financing requirements. This budget is important in ensuring an organization's solvency, maximizing returns from cash balances, and determining whether the organization is generating enough cash for current and future operations.
- **Cash disbursements budget.** This budget is dependent on the pattern of payments for expenses. Cash disbursements typically do not match costs in a period, since expenses generally are paid later than they are incurred.
- **Cash receipts budget.** The collection of sales depends on an organization's credit policies and its customer base. Most organizations must obtain cash to pay current bills while waiting for payment from customers. This cash represents an opportunity cost to the organization.

- **Labor budget.** This budget may be broken down by type of worker required in hours or number of workers.
- **Production cost budget.** This budget may be broken down by product or plant.
- **Production budget.** This budget may be broken down by product or plant. Production must meet current sales demand and maintain sufficient inventory levels for expected activity levels during the budget period and on into the next period. This budget is reviewed with the production managers to determine if it is realistic. If the budget is not attainable, management may revise the sales forecast or try to increase capacity. If production capacity will exceed requirements, other uses of the idle capacity may be considered.
- **Purchases budget.** This budget typically is broken down by raw materials and parts. An organization's inventory policy determines its level of purchases.
- **Sales budget.** This budget may be broken down by product, territory, plant, or other segment of interest.

(iv) Operating Budgeting Techniques

Budgets are a necessary component of financial decision making because they help provide an efficient allocation of resources. A budget is a profit-planning and a resource-controlling tool. It is a quantitative expression of management's intentions and plans for the coming year(s) to meet goals and objectives within the resource constraints. Budgets are prepared at the beginning of each year. Departmental or functional budgets are summarized and compared with revenue forecasts and revised as necessary.

Five budgeting techniques are available:

1. Incremental budgeting
2. Flexible budgeting
3. Zero-based budgeting
4. Program planning budgeting
5. Planning, programming, and budgeting systems

(See Exhibit 7.56.) A brief description of each budget is presented next.

1. Incremental budgeting (adds a percentage or fixed amount to the previous budget)
2. Flexible budgeting (reflects variation in activity levels)
3. Zero-based budgeting (uses decision packages to specify objectives and workloads)
4. Program planning budgeting (presents budget choices more explicitly in terms of objectives)
5. Planning, programming, and budgeting systems (link performance levels with specific budget amounts)

EXHIBIT 7.56 Budgeting Techniques

Incremental budgeting is a traditional approach to budgeting focusing on incremental changes in detailed categories of revenues and expenses, called line items, to represent sales, salaries, travel, supplies, and so forth. The incremental approach to budgeting does not take into account variation in volume or change in activity levels. It operates on the principle of management by exception.

Flexible budgeting (variable or dynamic budgeting) adjusts the budget for changes in the unit level of the cost or revenue. It is also called a variable budget. The flexible budget is based on the knowledge of how revenues and costs should behave over a range of activity. Thus, it is appropriate for any relevant level of activity. The master budget is not adjusted after it is developed, regardless of changes in volume, cost, or other conditions during the budget period.

Zero-based budgeting, especially in the public sector, attempts to analyze the incremental change in a program's output at different levels of funding. For each program, a decision package specifies objectives and measures of efficiency, effectiveness, and workload for alternate levels of funding.

Planning, programming, and budgeting systems (PPBS) attempt to further advance budgeting techniques, especially in the public sector, by presenting budget choices more explicit in terms of public objectives. With PPBS budgets, the cost and effectiveness of programs are evaluated in a multiyear framework, and alternate approaches are considered.

Performance budgeting, which also focuses on the public sector, links performance measures directly to agency missions and program objectives. Under the performance budgeting model, budgets are developed based on unit costs and service expectations followed by analysis of actual work performed compared with budget estimates.

BUDGET PURPOSES

The main purpose of a budget is to forecast and control the expenditures for a certain activity. A budget is an aid to planning and control. It helps managers to allocate resources efficiently and to achieve objectives effectively. A budget does not allow managers to estimate a firm's beta coefficient, which is a measure of stock market volatility.

(v) Advantages of Operating Budgets

Budgets are commonly used in both large and small organizations. No matter what the size of the organization, the benefits of budgeting typically exceed the costs. The **advantages** of budgets are listed next.

- Budgets compel planning. Management must have targets, and budgets reflect expected performance. Budgets affect strategies, which are the relatively general and permanent plans of an organization that change as conditions and/or objectives change. Budgets can give direction to operations, point out problems, and give meaning to results.
- **Budgets provide performance criteria.** The budget allows employees to know what is expected of them. Comparing actual results to budgeted amounts instead of past performance provides more useful information. Comparison with past performance may be hampered by past inefficiencies or changes in technology, personnel, products, or general economic conditions.
- **Budgets promote communication and coordination.** Coordination deals with the interests of the organization as a whole, meshing and balancing the factors of production and other departments and functions so that objectives can be achieved. Budgets aid coordination because they require well-laid plans and isolate any problems.

(vi) Limitations of Operating Budgeting Techniques

Peculiarities and limitations of budgets include:

- Budgeted items are a mixture of fixed and variable cost components. Accordingly, mixed costs cannot be used for linear projection.
- Budgeted items include some direct costs and some allocated costs. Direct costs are more useful for decision making than allocated costs. Responsibility accounting favors direct and controllable costs, not allocated and uncontrollable costs.
- The nature of volume levels needs to be understood. Most budgets are based on a single level of volume (point estimates), but multiple volume levels (range estimates) would be better for decision making.
- The kinds of assumptions made during the budget development process need to be known. One must understand the budget preparer's state of mind: optimistic, most likely, or pessimistic outcomes. Each of these outcomes would bring a different type of realism to the budget numbers.
- The variances from budgets need to be analyzed very carefully. Performance reports show the variations between the actual and the budgets—an element of control. Corrective action requires determination of underlying causes of variation. Variation could be favorable or unfavorable.

7.3 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. A company uses straight-line depreciation for financial reporting purposes, but uses accelerated depreciation for tax purposes. Which of the following account balances would be **lower** in the financial statements used for tax purposes than it would be in the general purpose financial statements?

a. Accumulated depreciation

b. Cash

c. Retained earnings

d. Gross fixed assets

2. Under a defined contribution pension plan, (List A) is reported on the balance sheet only if the amount the organization has contributed to the pension trust is (List B) the amount required.

	List A	List B
a.	An asset	Greater than
b.	An asset	Equal to
c.	A liability	Greater than
d.	A liability	Equal to

3. When a business is acquired, the purchasing company calculates goodwill associated with the acquisition as the difference between the purchase price and the:

a. Book value of the identifiable net assets acquired.

b. Fair market value of the identifiable net assets acquired.

c. Book value of the net tangible assets acquired.

d. Fair market value of the net tangible assets acquired.

4. What conclusion should a financial analyst draw if a company has a high fixed assets turnover ratio?

a. The company may be overcapitalized.

b. The company may have a problem with employees converting inventory to personal use.

c. The company may be undercapitalized.

d. The company has favorable profitability.

5. A company will finance next year's capital projects through debt rather than additional equity. The benchmark cost of capital for these projects should be:

a. The before-tax cost of new debt financing.

b. The after-tax cost of new debt financing.

c. The cost of equity financing.

d. The weighted-average cost of capital.

6. In the distribution of liquidation proceeds for a bankrupt firm, which of the following claimants has **highest** priority?

a. Preferred stock

b. Common stock

c. Bonds payable

d. Taxes payable

7. A company has a foreign-currency-denominated trade payable due in 60 days. In order to eliminate the foreign exchange risk associated with the payable, the company could:

a. Sell foreign currency forward today.

b. Wait 60 days and pay the invoice by purchasing foreign currency in the spot market at that time.

c. Buy foreign currency forward today.

d. Borrow foreign currency today, convert it to domestic currency on the spot market, and invest the funds in a domestic bank deposit until the invoice payment date.

8. The following information pertains to a checking account of a company at July 31, 20X2:

Balance per bank statement	$40,000
Interest earned for July	100
Outstanding checks	3,000
Customers' checks returned or insufficient funds	1,000
Deposit in transit	5,000

At July 31, 20X2, the company's correct cash balance is:

a. $41,100.

b. $41,000.

c. $42,100.

d. $42,000.

9. An organization borrows funds from its bank for a one-year period. The bank charges interest at a nominal rate of 15% per annum, on a discount basis, and requires a 10% compensating balance. The effective annual interest rate on the loan is:

a. 16.67%.

b. 17.65%.

c. 20.00%.

d. 25.00%.

10. The cost of materials has risen steadily over the year. The company uses its newest materials first when removing items from inventory. Which of the following methods of estimating the ending balance of the materials inventory account will result in the **highest** net income, all other variables held constant?

a. Last in, first out (LIFO).

b. First in, first out (FIFO).

c. Weighted average.

d. Specific identification.

11. General sales taxes tend to be regressive with respect to income because:

a. A larger portion of a poor person's income is subject to the tax.

b. A smaller portion of a poor person's income is subject to the tax.

c. The tax rate is higher for the poor.

d. The tax claims an increasing amount of income as income rises.

12. During the current accounting period, a manufacturing company purchased $70,000 of raw materials, of which $50,000 of direct materials and $5,000 of indirect materials was used in production. The company also incurred $45,000 of total labor costs and $20,000 of other factory overhead costs. An analysis of the work-in-process control account revealed $40,000 of direct labor costs. Based on the above information, what is the total amount accumulated in the factory overhead control account?

a. $25,000

b. $30,000

c. $45,000

d. $50,000

13. A company experienced a machinery breakdown on one of its production lines. As a consequence of the breakdown, manufacturing fell behind schedule, and a decision was made to schedule overtime in order to return manufacturing to schedule. Which one of the following methods is the proper way to account for the overtime paid to the direct laborers?

a. The overtime hours times the sum of the straight-time wages and overtime premium would be charged entirely to manufacturing overhead.

b. The overtime hours times the sum of the straight-time wages and overtime premium would be treated as direct labor.

c. The overtime hours times the overtime premium would be charged to repair and maintenance expense while the overtime hours times the straight-time wages would be treated as direct labor.

d. The overtime hours times the overtime premium would be charged to manufacturing overhead while the overtime hours times the straight-time wages would be treated as direct labor.

14. A company has analyzed seven new projects, each of which has its own internal rate of return (IRR). It should consider each project whose internal rate of return is _____ its marginal cost of capital (MCC) and accept those projects in _____ order of their IRR.

a. Below; decreasing.

b. Above; decreasing.

c. Above; increasing.

d. Below; increasing.

15. An existing machine with estimated remaining life of five years that cost $100,000 can be sold for $20,000. The variable cost of output from this machine has been $1 per unit with 100,000 units per year produced. A new machine will cost $90,000 and is estimated to lower the variable cost to $.70 per unit over its five-year life. The most appropriate term for the decision process involved in this scenario is:

a. Capital budgeting.

b. Economic order quantity.

c. Flexible budgeting.

d. Sensitivity analysis.

16. Many service industries utilize a budgeting process to identify major programs and develop short-term operating budgets, such as expected revenues and expected direct expenses, for the identified programs. For example, a nursing home may develop one-year revenue and expense budgets for each of its different programs, such as day care for the elderly or Meals on Wheels. Which of the following is a **major** advantage of short-term program planning and budgeting?

a. It eliminates the need for periodic program evaluation.

b. It provides a rigid basis for periodic program evaluation.

c. It promotes communication and coordination within an organization.

d. It provides an important basis for strategic analysis of the goals of the organization.

17. Actual and projected sales of a company for September and October are:

	Cash sales	Credit sales
September (actual)	$20,000	$50,000
October (projected)	30,000	55,000

All credit sales are collected in the month following the month in which the sale is made. The September 30 cash balance is $23,000. Cash disbursements in October are projected to be $94,000. To maintain a minimum cash balance of $15,000 on October 31, the company will need to borrow:

a. $0.

b. $ 6,000.

c. $11,000.

d. $16,000.

18. Which of the following is **not** true about international transfer prices for a multinational firm?

a. They allow firms to attempt to minimize worldwide taxes.

b. They allow the firm to evaluate each division.

c. They provide each division with a profit-making orientation.

d. They allow firms to correctly price products in each country in which they operate.

19. One department of an organization, Final Assembly, is purchasing subcomponents from another department, Materials Fabrication. The price that Materials Fabrication will charge Final Assembly is to be determined. Outside market prices for the subcomponents are available. Which of the following is the **most correct** statement regarding a market-based transfer price?

a. Marginal production cost transfer prices provide incentives to use otherwise idle capacity.

b. Market transfer prices provide an incentive to use otherwise idle capacity.

c. Overall long-term competitiveness is enhanced with a market-based transfer price.

d. Corporate politics is more of a factor in a market-based transfer price than with other methods.

20. A company makes a product that sells for $30. During the coming year, fixed costs are expected to be $180,000, and variable costs are estimated at $26 per unit. How many units must the company sell in order to break even?

a. 6,000

b. 6,924

c. 45,000

d. 720,000

21. In its first year of operations, a firm had $50,000 of fixed operating costs. It sold 10,000 units at a $10 unit price and incurred variable costs of $4 per unit. If all prices and costs will be the same in the second year and sales are projected to rise to 25,000 units, what will the degree of operating leverage (the extent to which fixed costs are used in the firm's operations) be in the second year?

a. 1.25

b. 1.50

c. 2.00

d. 6.00

22. A company has 7,000 obsolete toys, which are carried in inventory at a manufacturing cost of $6 per unit. If the toys are reworked for $2 per unit, they could be sold for $3 per unit. If the toys are scrapped, they could be sold for $1.85 per unit. Which alternative is more desirable (rework or scrap), and what is the total dollar amount of the advantage of that alternative?

a. Scrap, $5,950

b. Rework, $36,050

c. Scrap, $47,950

d. Rework, $8,050

23. Which of the following statements about activity-based costing (ABC) is **not** true?

a. ABC is useful for allocating marketing and distribution costs.

b. ABC is more likely to result in major differences from traditional costing systems if the firm manufactures only one product rather than multiple products.

c. In ABC, cost drivers are what cause costs to be incurred.

d. ABC differs from traditional costing systems in that products are not cross-subsidized.

24. The following information is available from the records of a manufacturing company that applies factory overhead based on direct labor hours:

Estimated overhead cost	$500,000
Estimated labor hours	200,000 hours
Actual overhead cost	$515,000
Actual labor hours	210,000 hours

Based on this information, overhead would be:

a. Underapplied by $9,524.

b. Overapplied by $10,000.

c. Overapplied by $15,000.

d. Overapplied by $40,750.

25. A company plans to implement a bonus plan based on segment performance. In addition, the company plans to convert to a responsibility accounting system for segment reporting. The following costs, which have been included in the segment performance reports that have been prepared under the current system, are being reviewed to determine if they should be included in the responsibility accounting segment reports.

1. Corporate administrative costs allocated on the basis of net segment sales
2. Personnel costs assigned on the basis of the number of employees in each segment
3. Fixed computer facility costs divided equally among each segment
4. Variable computer operational costs charged to each segment based on actual hours used times a predetermined standard rate; any variable cost efficiency or inefficiency remains in the computer department

Of these four cost items, the only item that could logically be included in the segment performance reports prepared on a responsibility accounting basis would be the:

a. Corporate administrative costs.

b. Personnel costs.

c. Fixed computer facility costs.

d. Variable computer operational costs.

DOMAIN 8

Global Business Environment (0–10%)

8.1 Economic/Financial Environments

Topics such as organization structures, types of international strategies, international strategic and tactical objectives, technology and global strategy, and forms of international business and marketing strategies are presented in this section.

(a) Organization Structures

The organization structure of the multinational corporation (MNC) evolves over time due to changes in economic policies, tax laws, government regulations, and political structures. The organizational structure of the MNC varies; each manager's level has a varied degree of authority and responsibility.

MNCs are firms with significant foreign direct investment assets. They are characterized by their ability to derive and transfer capital resources worldwide and to operate facilities of production and penetrate markets in more than one country, usually on a global scale. Over the past 30 years, many writers have argued over the best name to use in referring to these companies. "Multinational enterprise" (MNE) has been a popular term because it reflects the fact that many global firms are not, technically speaking, "corporations." The terms "transnational corporation" and "supranational corporation" are often used within the United Nations system, where many internationalists argue that the operations and interests of the modern corporation "transcend" national boundaries.

One significant trend in business during the last half of the twentieth century has been the globalization of MNCs. At one time, MNCs were simply large domestic companies with foreign operations. Today, they are global companies. They typically make decisions and enter strategic alliances with each other without regard to national boundaries. They move factories, technology, and capital to those countries with the most hospitable laws, the lowest tax rates, the most qualified

workforce, or abundant natural resources. They see market share and company performance in global terms. Foreign sales and operations are extremely profitable for many multinationals.

Mueller and his co-authors[1] suggest five common forms of organizations used by MNCs:

1. International division/department
2. Organization by product line
3. Functional organization
4. Geographic organization
5. Global matrix organization

(See Exhibit 8.1.)

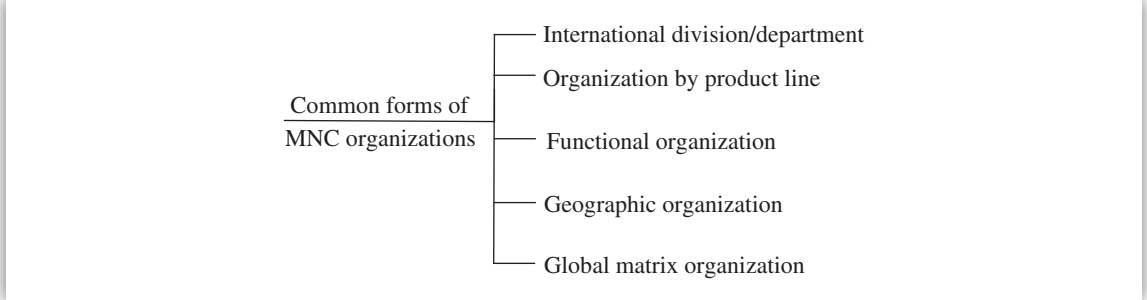


EXHIBIT 8.1 Common Forms of MNC Organizations

The **international division/department** separates foreign operations from domestic operations. This international division is usually evaluated as an independent operation and compared with the domestic division. **Organization by product line** results in the integration of domestic and foreign operations and the evaluation of product lines based on worldwide results.

A company **grouped by function** (such as marketing, manufacturing, or accounting) is called a functional organization, and management maintains centralized control over the functions. An example is that the vice president for marketing or manufacturing at U.S. headquarters would be responsible for the marketing or manufacturing function worldwide. This structure is not common but is popular among oil and coal companies whose products are homogeneous.

Geographic organization separates operations into geographic areas such as North America, Europe, and Asia. A company would use this form of structure when it has substantial foreign operations that are not dominated by a particular country or area of the world. U.S. MNCs do not use this form as often as European and Japanese MNCs do because U.S. MNCs are usually dominated by their domestic markets.

The **global matrix organization** blends two or more of the four forms just presented. An example is that the general manager of a German subsidiary will report to the vice president for worldwide product lines and to the area vice president for Europe. The matrix organization avoids the problems inherent in either integrating or separating foreign operations.

[1] Gerhard G. Mueller, Helen Morsicato Gernon, and Gary K. Meek, *Accounting: An International Perspective*, 3rd ed. (Burr Ridge, IL: Irwin, 1994).

(i) Information Flows and Organization Structures of MNCs

The following list provides guidelines for information flows and organization structures of MNCs.

- Within the international division or department, information flows from subsidiaries to the vice president of the international division.
- In MNCs organized by product line, information flows from subsidiaries to the vice president of the product line.
- In an MNC organized by function, information flows from subsidiary to headquarters according to specific business function (i.e., marketing, manufacturing, or accounting).
- When MNCs are geographically organized, the subsidiary information is collected within a geographic area and then sent to headquarters.
- With the matrix form, information flows in two directions: from the subsidiary to the geographic location headquarters and by product line to MNC headquarters.

(ii) Models of Multinational Business

Another dimension to the organization of MNCs is the attitude of headquarters management toward multinational business. These attitudes can be classified into three models: ethnocentric (home-country oriented), polycentric (host-country oriented), and geocentric (world oriented) (see Exhibit 8.2).

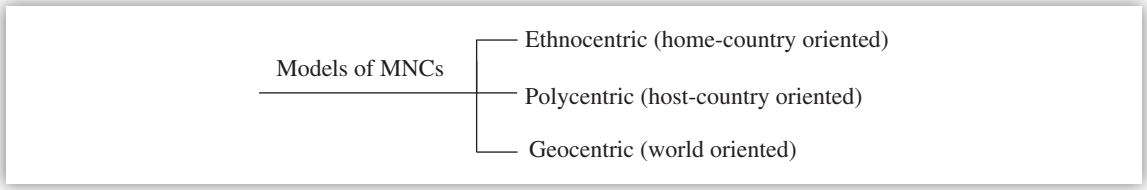


EXHIBIT 8.2 Models of MNCs

An **ethnocentric management** thinks that home-country standards are superior and therefore applies them worldwide. Automakers are an example of the ethnocentric management model. A **polycentric management** assumes that host-country cultures are different and, therefore, allows local subsidiaries or affiliates to operate autonomously. Standards for performance evaluation and control functions are determined locally. Pharmaceutical companies are an example of the polycentric model.

A **geocentric management** focuses on worldwide objectives and considers foreign subsidiaries as part of a whole. Standards for performance evaluation and control functions are determined both universally and locally. It is an ideal model where decisions are considered globally while, at the same time, individual subsidiaries are able to respond to the demands of host governments and the local customer. People of many different nationalities serve on the board of directors and senior management teams. N.V. Philips and Unilever are good examples of the geocentric management model. "*Think globally and act locally" is the basic tenet of corporations that are geocentrically managed.*

The "host country" refers to that nation in which an MNC establishes a subsidiary in a local country. The "home country" (parent country) refers to that nation in which an MNC establishes a subsidiary in a foreign country.

The attitudes of headquarters management also affect the location of decision making. Basically, three types of decision making may result: centralized, decentralized, and semicentralized or semidecentralized (see Exhibit 8.3).

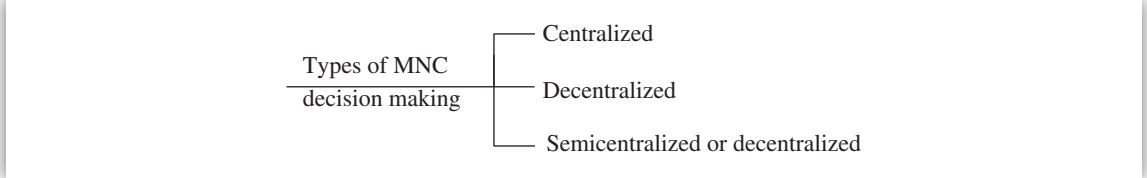


EXHIBIT 8.3 Types of MNC Decision Making

If decision-making authority rests with headquarters, an MNC is said to be **centralized**. Even with this structure, an MNC generally does not make all decisions at one location but aims for a collaborative approach between headquarters and other business units.

If an MNC headquarters allows foreign subsidiaries to make important decisions, the corporation is considered to be **decentralized**. This structure is more common when global diversity is considered. Managers of foreign subsidiaries are allowed a great deal of autonomy to plan, control, and evaluate their own operations at the local level.

Not all MNCs are purely centralized or decentralized. Often a mixture of organizations is necessary. **Semicentralized or semidecentralized** decision making arises when an MNC centralizes functions considered critical for success (e.g., research and development [R&D]) and decentralizes those that are less critical (e.g., marketing, production).

(b) Types of International Strategies

International firms typically develop their core strategy for the home country first. Subsequently, they internationalize their core strategy through international expansion of activities and through adaptation. Eventually, they globalize their strategy by integrating operations across nations. These steps translate into four distinct types of strategies applied by international enterprises: (1) ethnocentric, (2) multidomestic, (3) global, and (4) transnational.

(i) Ethnocentric Strategy

Following World War II, U.S. enterprises operated mainly from an **ethnocentric** perspective. These companies produced unique goods and services, which they offered primarily to the domestic market. The lack of international competition offset the need of these enterprises to be sensitive to cultural differences. When these firms exported goods, they did not alter them for foreign consumption—the costs of alterations for cultural differences were assumed by the foreign buyers. In effect, this type of company had one strategy for all markets.

(ii) Multidomestic Strategy

The multidomestic firm has a different strategy for each of its foreign markets. In this type of strategy, "a company's management tries to operate effectively across a series of worldwide positions with diverse product requirements, growth rates, competitive environments, and political risks. The company prefers that local managers do what is necessary to succeed in

R&D, production, marketing, and distribution, but holds them responsible for results."[2] In essence, this type of corporation competes with local competitors on a market-by-market basis.

(iii) Global Strategy

The **global corporation** uses all of its resources against its competition in a very integrated fashion. All of its foreign subsidiaries and divisions are highly interdependent in both operations and strategy. Therefore, whereas in a multidomestic strategy, the managers in each country react to competition without considering what is taking place in other countries, in a global strategy, competitive moves are integrated across nations. The same kind of move is made in different countries at the same time or in a systematic fashion. For example, a competitor is attacked in one nation in order to exhaust its resources for another country, or a competitive attack in one nation is countered in a different country—in that instance, the counterattack in a competitor's home market is a parry to an attack on one's home market.

The advantages of the global strategy would negate the disadvantages of the multidomestic strategy, and the disadvantages of the global strategy would be negated by the advantages of the multidomestic strategy.

ADVANTAGES AND DISADVANTAGES OF GLOBAL STRATEGY

Advantages

(Multidomestic strategy does not provide these advantages.)

- By pooling production or other activities for two or more nations, a firm can increase the benefits derived from economies of scale.
- A company can cut costs by moving manufacturing or other activities to low-cost countries.
- A firm that is able to switch production among different nations can reduce costs by increasing its bargaining power over suppliers, workers, and host governments.
- By focusing on a smaller number of products and programs than those under a multidomestic strategy, a corporation is able to improve both product and program quality.
- Worldwide availability, serviceability, and recognition can increase preference through reinforcement.
- The company is provided with more points from which to attack and counterattack competition.

Disadvantages

(Multidomestic strategy can reduce these disadvantages.)

- Through increased coordination, reporting requirements, and added staff, substantial management costs can be incurred.
- Overcentralization can harm local motivation and morale, thus reducing the firm's effectiveness.
- Standardization can result in a product that does not totally satisfy any customers.
- Incurring costs and revenues in multiple countries increases currency risk.
- Integrated competitive moves can lead to the sacrificing of revenues, profits, or competitive positions in individual countries—especially when the subsidiary in one country is told to attack a global competitor in order to convey a signal or divert that competitor's resources from another nation.

[2] Jack Craig, *Multinational Cooperatives: An Alternative for World Development* (Saskatoon, Saskatchewan, Canada: Western Producers Prairie Books, 1976).

(iv) Transnational Strategy

The **transnational strategy** provides for global coordination (like the global strategy) and, at the same time, it allows local autonomy (like the multidomestic strategy). Nestlé, the world's largest food company, headquartered in Switzerland, follows this strategy. The challenges managers of transnational corporations face are to identify and exploit cross-border synergies and to balance local demands with the global vision for the corporation. Building an effective transnational organization requires a corporate culture that values global dissimilarities across cultures and markets.

KEY CONCEPTS TO REMEMBER: Profile of Transnational Enterprises

- A transnational enterprise is an MNC doing business globally to take advantage of tax incentives and to develop collaborative relations with foreign trading firms. Dr. Jack Craig of Canada's York University[a] summarized the evolution of transnational enterprises as follows: from ethnocentric to polycentric to geocentric, and from profit-oriented and investor-oriented firms to joint ventures to mixed orientations.
- From ethnocentric with complex organization in the home country; centralized decision making in headquarters evaluation and control of performance based on the home-country standards; communication flow outward to subsidiaries in host countries that have simpler organizations; ownership and recruitment of key management largely of home nationality.
- To polycentric with varied and independent organization; less headquarters authority and decision making; evaluation and control determined locally; wide variations in performance management and standards depending on local cultures; limited communication to/from headquarters and among subsidiaries; ownership, key management, and recruitment from host country.
- To preferred geocentric with increasingly complex, interdependent organization; seeking a collaborative approach between and among headquarters/subsidiaries; uses standards for evaluation and control that are both universal and local; international and local executives rewarded for reaching both local and worldwide objectives; ownership, key management, and recruitment is cosmopolitan—to develop the best person anywhere is the major criterion.
- From profit-oriented and investor-owned corporations with direct investments in foreign subsidiaries and joint ventures or consortia, to mixed orientations (government-owned to service-owned cooperatives).

[a] Jack Craig, *Multinational Cooperatives: An Alternative for World Development* (Saskatoon, Saskatchewan, Canada: Western Producers Prairie Books), 1976.

(c) International Strategic and Tactical Objectives

Organizations generally establish two kinds of measurable objectives: strategic and tactical. **Strategic objectives**, which are guided by the enterprise's mission or purpose and deal with long-term issues, associate the enterprise to its external environment and provide management with a basis for comparing performance with that of its competitors and in relation to environmental demands. Examples of strategic objectives include to increase sales, to increase market share, to increase profits, and to lower prices by becoming an international firm. **Tactical objectives**, which are guided by the enterprise's strategic objectives and deal with shorter-term issues, identify the key result areas in which specific performance is essential for the success

of the enterprise and aim to attain internal efficiency. For example, they identify specifically how to lower costs, lower prices, increase output, capture a larger portion of the market, and penetrate an international market.

(d) Technology and Global Strategy

Technology has been at the root of the most dramatic changes occurring in commerce today. It now enables organizations to integrate their systems, where changes in one part ripple throughout the system, causing shifts in the other parts. Therefore, no strategy has been left untouched. Technology has leveled the playing field for small firms, allowing them to compete successfully with large corporations in the same markets. With e-mail, videoconferencing, multimedia CD-ROMs, and networked databases, small businesses can emulate the marketing tactics of much larger companies—they can set up a home page on the World Wide Web right next door to Walmart. And electronic networks and the Internet have enabled organizations to decentralize business activities and to outsource activities to other organizations.

From a strategic viewpoint, technology has impacted international strategy in several important ways.

- Emphasis has moved from products to information and solutions.
- Products can be launched from commercialization tactics based on identifying specific customer needs.
- Relationships with customers have been made easier, which enhances product acceptance and minimizes costs due to redesign.
- Firms can now target specific products and services to specific customers.
- Technology supports the integration of engineering and commercialization to get the product to the customer in the least amount of time.
- Technology helps prevent midcourse corrections in product design, which usually result in higher costs and longer time to commercialize.

From a tactical viewpoint, current technology aids businesses in the commercialization of their products and services in numerous ways.

- E-mail enables firms to communicate rapidly and easily with customers, strategic partners, suppliers, distributors, and others around the globe. This lowers the costs of travel and speeds up response time.
- Videoconferencing allows enterprises to hold international strategic meetings without getting on an airplane.
- Networked databases provide organizations with online access to R&D information existing around the globe.
- Internet access and laptop computers let employees work from virtually anywhere in the world, increasing efficiency and bringing the organization closer to the customer.
- Satellite systems, which a firm can lease from a provider, allow organizations to receive broadcast messages from chain manufacturers that help move the product.

- Laser color printers allow enterprises to quickly produce signs, banners, cards, price tags, and so on that look as good as those printed by a professional.
- Some industries have CD-ROM services that businesses can tie into on a regular basis to receive updated information of things such as equipment and supplies. This also makes it easier for a firm to quickly locate customer items that it normally does not carry in stock.
- The World Wide Web as a commercial tool is enabling smaller businesses to be on the same playing field as larger businesses.
- Online databases have put information in the hands of anyone who chooses to access them.

One must bear in mind that **technology is a tool used by strategists to improve business activities**. It is not intended to replace personal contact with the customer, nor is it intended to replace a manager's unique ability to take vast amounts of information and make sense of it in terms of strategy for the organization. It does make it easier for the manager to integrate all activities of the firm, automate routine tasks, and generally free up more time to focus on the firm's strategy.

(e) Forms of International Business and Marketing Strategies

We classify international business into three categories: trade, intellectual property rights (trademarks, patents, and copyrights) and international licensing agreements, and foreign direct investment. To the marketer, these broad categories describe three important methods for entering a foreign market. To the lawyer, they also represent the form of doing business in a foreign country and the legal relationship between parties to a business transaction. Each method brings a different set of problems to the firm because the level of foreign penetration and entanglement in various countries is different. Trade usually represents the least entanglement and, thus, the least political, economic, and legal risk, especially if the exporting firm is not soliciting business overseas or maintaining sales agents or inventories there. An investment in a plant and operations overseas usually represents the greatest market penetration and, thus, the greatest risk to the firm.

Considerable overlap occurs among these different forms of doing business. A business plan for the production and marketing of a single product may contain elements of each form. To illustrate, a U.S. firm might purchase the rights to a trademark for use on an article of high-fashion clothing made from fabric exported from China and assembled in offshore plants in the Caribbean for shipment to the United States and Europe. Here a business strategy encompasses elements of trade, licensing, and investment. For firms just entering a new foreign market, the method of entry might depend on a host of considerations, including the sophistication of the firm, its overseas experience, the nature of its product or services, its commitment of capital resources, and the amount of risk it is willing to bear.

(i) Trade

Trade consists of the import and export of goods and services. "Exporting" is the term generally used to refer to the process of sending goods out of a country, and "importing" is used to denote when goods are brought into a country. However, a more accurate definition is that *exporting is the shipment of goods or the rendering of services to a foreign buyer located in a foreign country. Importing* is then defined as *the process of buying goods from a foreign supplier and entering them into the customs territory of a different country.* Every export entails an import, and vice versa.

(A) Exporting Trade is often a firm's first step into international business. Compared to the other forms of international business (licensing and investment), trade is relatively uncomplicated. It provides the inexperienced or smaller firm with an opportunity to penetrate a new market, or at least to explore foreign market potential, without significant capital investment and the risks of becoming a full-fledged player (i.e., citizen) in the foreign country. For many larger firms, including MNCs, exporting may be an important portion of their business operations. The U.S. aircraft industry, for example, relies heavily on exports for significant revenues.

Firms that have not done business overseas before should first prepare an export plan, which can mean assembling an export team, composed possibly of management and outside advisors and trade specialists. Their plan should include the assessment of the firm's readiness for exporting, the export potential of its products or services, the firm's willingness to allocate resources (including financial, production output, and human resources), and the selection of its channels of distribution. The firm may need to modify products, design new packaging and foreign-language labeling, and meet foreign standards for product performance or quality assurance. The firm must also gauge the extent to which it can perform export functions in-house or whether these functions should best be handled indirectly through an independent export company. Export functions include foreign marketing, sales and distribution, shipping, and handling international transfers of money.

Firms accept varying levels of responsibility for moving goods and money and for other export functions. The more experienced exporters can take greater responsibility for themselves and are more likely to export directly to their foreign customers. Firms that choose to accept less responsibility in dealing with foreign customers or in making arrangements for shipping, for example, must delegate many export functions to someone else. As such, exporting is generally divided into two types: direct and indirect.

At first glance, **direct exporting** seems similar to selling goods to a domestic buyer. A prospective foreign customer may have seen a firm's products at a trade show, located a particular company in an industrial directory, or been recommended by another customer. A firm that receives a request for product and pricing information from a foreign customer may be able to handle it routinely and export directly to the buyer. With some assistance, a firm can overcome most hurdles, get the goods properly packaged and shipped, and receive payment as anticipated. Although many of these onetime sales are turned into long-term business success stories, many more are not. A firm hopes to develop a regular business relationship with its new foreign customer. However, the problems that can be encountered even in direct exporting are considerable.

Many firms engaged in direct exporting on a regular basis reach the point at which they must hire their own full-time export managers and international sales specialists. These people participate in making export-marketing decisions, including product development, pricing, packaging, and labeling for export. They should take primary responsibility for dealing with foreign buyers, attending foreign trade shows, complying with government export and import regulations, shipping, and handling the movement of goods and money in the transaction. Direct exporting is often done through **foreign sales agents** who work on commission. It also can be done by selling directly to **foreign distributors**. Foreign distributors are independent firms, usually located in the country to which a firm is exporting, that purchase goods for resale to their customers. They assume the risks of buying and warehousing goods in their market and provide additional product support services. These distributors usually service the products they sell, thus relieving the exporter of that responsibility. They often train end users to use the product, extend credit to their customers, and bear responsibility for local advertising and promotion.

Indirect exporting is used by companies seeking to minimize their involvement abroad. Lacking experience, personnel, or capital, they may be unable to locate foreign buyers or are not yet ready to be handling the mechanics of a transaction on their own. There are several different types of indirect exporting. **Export trading companies**, commonly called ETCs, are companies that market the products of several manufacturers in foreign markets. They have extensive sales contacts overseas and experience in air and sea shipping. They often operate with the assistance and financial backing of large banks, thus making the resources and international contacts of the bank's foreign branches available to the manufacturers whose products they market. ETCs are licensed to operate under the U.S. antitrust laws.

Export management companies (EMCs), however, are really consultants that advise manufacturers and other exporters. Firms that cannot justify their own in-house export managers use them. They engage in foreign market research, identify overseas sales agents, exhibit goods at foreign trade shows, prepare documentation for export, and handle language translations and shipping arrangements. As in direct exporting, all forms of indirect exporting can involve sales through agents or to distributors.

(B) Importing and Global Sourcing Here importing is presented from the perspective of the global firm for which importing is a regular and necessary part of their business. **Global sourcing** is the term commonly used to describe the process by which a firm attempts to locate and purchase goods or services on a worldwide basis. These goods may include, for example, raw materials for manufacturing, component parts for assembly operations, commodities such as agricultural products or minerals, or merchandise for resale.

(C) Government Controls over Trade: Tariffs and Nontariff Barriers Both importing and exporting are governed by the laws and regulations of the countries through which goods or services pass. Nations regulate trade in many ways. The most common methods are **tariffs** and **nontariff barriers**. Tariffs are import duties or taxes imposed on goods entering the customs territory of a nation. Tariffs are imposed for many reasons, including the collection of revenue, the protection of domestic industries from foreign competition, and political control (e.g., to provide incentives to import products from politically friendly countries and to discourage importing products from unfriendly countries).

Nontariff barriers are *all barriers to importing or exporting other than tariffs.* Nontariff barriers are generally a greater barrier to trade than are tariffs because they are more insidious. Unlike tariffs, which are published and easily understood, nontariff barriers are often disguised in the form of government rules or industry regulations and often are not understood by foreign companies. Countries impose nontariff barriers to protect their national economic, social, and political interests. Imports might be banned for health and safety reasons. Imported goods usually have to be marked with the country of origin and labeled in the local language so that consumers know what they are buying. One form of nontariff barrier is the **technical barrier to trade**, or **product standard**. Examples of product standards include safety standards, electrical standards, and environmental standards (e.g., German cars meeting U.S. emission standards not mandated in Europe). A **quota** is a restriction imposed by law on the numbers or quantities of goods, or of a particular type of good, allowed to be imported. Unlike tariffs, quotas are not internationally accepted as a lawful means of regulating trade except in some special cases. An **embargo** is a total or near-total ban on trade with a particular country, sometimes enforced by military action and usually imposed for political purposes. An internationally orchestrated embargo was used against Iraq after its invasion of Kuwait in 1990. A **boycott** is a refusal to trade or do business with certain firms, usually from a particular country, on political or other grounds.

Tariffs and nontariff barriers have a tremendous influence on how firms make their trade and investment decisions. These decisions, in turn, are reflected in the patterns of world trade and the flows of investment capital.

(D) Trade Liberalization and the World Trade Organization **Trade liberalization** refers to the efforts of governments to reduce tariffs and nontariff barriers to trade. In the twentieth century, the most important effort to liberalize trade came with the international acceptance of the **General Agreement on Tariffs and Trade (GATT)**. This is an agreement between nations, first signed in 1947 and continually expanded since that time, that sets the rules for how nations will regulate international trade in goods and services. In 1995, the Geneva-based **World Trade Organization (WTO)**, was created to administer the rules and to assist in settling trade disputes between its member nations. All WTO nations are entitled to **normal trade relations** with one another. This is referred to as **most favored nation (MFN)** trading status. This means that a member country must charge the same tariff on imported goods, and not a higher one, as that charged on the same goods coming from other WTO member countries. Trade liberalization has led to increased economic development and an improved quality of life around the world.

Another type of restriction over trade is export control. An **export control** limits the type of product that may be shipped to any particular country. These controls usually are imposed for economic or political purposes and are used by all nations of the world. For instance, high-tech computers might not be allowed to be shipped from the United States or Canada to another country without a license from the U.S. or Canadian government. Before signing a contract for the sale of certain products or technical know-how to a foreign customer, U.S. exporters must consider whether they will be able to obtain U.S. licensing for the shipment.

(ii) Intellectual Property Rights and International Licensing Agreements

Intellectual property (IP) rights are a grant from a government to an individual or firm of the exclusive legal right to use a copyright, patent, or trademark for a specified time. Copyrights are legal rights to artistic or written works, including books, software, films, music, or to such works as the layout design of a computer chip. Trademarks include the legal right to use a name or symbol that identifies a firm or its product. Patents are governmental grants to inventors assuring them of the exclusive legal right to produce and sell their inventions for a period of years. Copyrights, trademarks, and patents compose substantial assets of many domestic and international firms. As valuable assets, IP can be sold or licensed for use to others through a licensing agreement.

International licensing agreements are contracts by which the holder of IP will grant certain rights in that property to a foreign firm under specified conditions and for a specified time. Licensing agreements represent an important foreign market entry method for firms with marketable IP. For example, a firm might license the right to manufacture and distribute a certain type of computer chip or the right to use a trademark on apparel such as blue jeans or designer clothing. It might license the right to distribute Hollywood movies or to reproduce and market word-processing software in a foreign market, or it might license its patent rights to produce and sell a high-tech product or pharmaceutical. U.S. firms have extensively licensed their property around the world and in recent years have purchased the technology rights of Japanese and other foreign firms.

A firm may choose licensing as its market entry method because licensing can provide a greater entrée to the foreign market than is possible through exporting. A firm may realize many advantages in having a foreign company produce and sell products based on its IP instead of simply

shipping finished goods to that market. When exporting to a foreign market, the firm must overcome obstacles, such as long-distance shipping and the resulting delay in filling orders. Exporting requires a familiarity with the local culture. Redesign of products or technology for the foreign market may be necessary. Importantly, an exporter may have to overcome trade restrictions, such as quotas or tariffs, set by the foreign government. Licensing to a foreign firm allows the licensor to circumvent trade restrictions by having the products produced locally, and it allows entrance to the foreign market with minimal initial start-up costs. In return, the licensor might choose to receive a guaranteed return based on a percentage of gross revenues. This arrangement ensures payment to the licensor whether the licensee earns a profit or not. Even though licensing agreements give the licensor some control over how the licensee utilizes its IP, problems can arise. For instance, the licensor may find that it cannot police the licensee's manufacturing or quality control process. Protecting itself from the unauthorized use, or piracy, of its copyrights, patents, or trademarks by unscrupulous persons not party to the licensing agreement is also a serious concern for the licensor.

(A) Technology Transfer The exchange of technology and manufacturing know-how between firms in different countries through arrangements such as licensing agreements is known as technology transfer. Transfers of technology and know-how are regulated by government control in some countries. This control is common when the licensor is from a highly industrialized country, such as the United States, and the licensee is located in a developing country, such as those in Latin America, the Middle East, or Asia. In their efforts to industrialize, modernize, and develop a self-sufficiency in technology and production methods, these countries often restrict the terms of licensing agreements in a manner benefiting their own country. For instance, government regulation might require that the licensor introduce its most modern technology to the developing countries or train workers in its use.

(B) International Franchising Franchising is a form of licensing that is gaining in popularity worldwide. The most common form of franchising is known as a business operations franchise, usually used in retailing. Under a typical franchising agreement, the franchisee is allowed to use a trade name or trademark in offering goods or services to the public in return for a royalty based on a percentage of sales or other fee structure. The franchisee usually obtains the franchiser's know-how in operating and managing a profitable business and its other "secrets of success" (ranging from a "secret recipe" to store design to accounting methods). Franchising in the United States accounts for a large proportion of total retail sales. In foreign markets as well, franchising has been successful in fast food retailing, hotels, video rentals, convenience stores, photocopying services, and real estate services, to name but a few. U.S. firms have excelled in franchising overseas, making up the majority of new franchise operations worldwide. The prospects for future growth in foreign markets are enormous, especially in developing countries, such as those in Latin America. For instance, American fast food and retail franchises are common throughout Mexico City, Brazil, Eastern Europe, China, India and the former Soviet Union.

(C) Some Legal Aspects of Franchising Franchising is a good vehicle for entering a foreign market because the local franchisee provides capital investment, entrepreneurial commitment, and on-site management to deal with local customs and labor problems. However, many legal requirements affect franchising. Franchising in the United States is regulated primarily by the Federal Trade Commission (FTC) at the federal level. The agency requires the filing of extensive disclosure statements to protect prospective investors. Other countries have also enacted new franchise disclosure laws. Some developing countries have restrictions on the amount of money that can

be removed from the country by the franchiser. Moreover, some countries, such as China, also require government approval for franchise operations. Other countries might have restrictions on importing supplies (ketchup, bed linens, paper products, or whatever) for the operation of the business to protect local companies. However, more progressive developing countries are now abandoning these strict regulations because they want to welcome to their markets franchisers, their high-quality consumer products, and their managerial talent. Because of this more receptive attitude toward foreign firms, Mexico and Brazil have become home to many profitable new franchise operations.

(iii) Foreign Direct Investment

The term **foreign investment**, or **foreign direct investment**, refers to the ownership and active control of ongoing business concerns, including investment in manufacturing, mining, farming, assembly operations, and other facilities of production. A distinction is made between the home and host countries of the firms involved. The **home country** refers to that country under whose laws the investing corporation was created or is headquartered. For example, the United States is home to MNCs such as **Ford**, **Exxon**, and **IBM**, to name a few, but they operate in **host countries** throughout every region of the world. Of the three forms of international business, foreign investment provides the firm with the most involvement, and perhaps the greatest risk, abroad. Investment in a foreign plant is often a result of having had successful experiences in exporting or licensing, and of the search for ways to overcome the disadvantages of those other entry methods. For example, by producing its product in a foreign country instead of exporting, a firm can avoid quotas and tariffs on imported goods, avoid currency fluctuations on the traded goods, provide better product service and spare parts, and more quickly adapt products to local tastes and market trends. Manufacturing overseas for foreign markets can mean taking advantage of local natural resources, labor, and manufacturing economies of scale. Foreign investment in the United States is often called reverse investment. Most of the earlier foreign investment in the United States has come from the United Kingdom.

MNCs wishing to enter a foreign market through direct investment can structure their business arrangements in many different ways. Their options and eventual course of action may depend on many factors, including industry and market conditions, capitalization of the firm and financing, and legal considerations. Some of these options include the start-up of a new foreign subsidiary company, the formation of a joint venture with an existing foreign company, or the acquisition of an existing foreign company by stock purchase. For now, keep in mind that MNCs are usually not a single legal entity. They are global enterprises that consist of any number of interrelated corporate entities, connected through extremely complex chains of stock ownership. Stock ownership gives the investing corporation tremendous flexibility when investing abroad.

The **wholly owned foreign subsidiary** is a "foreign" corporation organized under the laws of a foreign host country but owned and controlled by the parent corporation in the home country. Because the parent company controls all of the stock in the subsidiary, it can control management and financial decision making.

The **joint venture** is a cooperative business arrangement between two or more companies for profit. A joint venture may take the form of a partnership or corporation. Typically, one party will contribute expertise and another the capital, each bringing its own special resources to the venture. Joint ventures exist in all regions of the world and in all types of industries. Where the laws of a host country require local ownership or that investing foreign firms have a local partner, the joint venture is an appropriate investment vehicle. **Local participation** refers to the requirement that a

share of the business be owned by nationals of the host country. These requirements are gradually being reduced in most countries that, in an effort to attract more investment, are permitting wholly owned subsidiaries. Many American companies do not favor the joint venture as an investment vehicle because they do not want to share technology, expertise, and profits with another company.

Another method of investing abroad is for two companies to **merge** or for one company to acquire another ongoing firm. This option has appeal because it requires less know-how than does a new start-up and can be concluded without disruption of business activity.

8.2 Cultural/Political Environments

In this section, topics such as different local/regional cultures, cross-cultural negotiations, and global mindsets are discussed.

(a) Different Local/Regional Cultures

Because it is so difficult to define precisely, many definitions of culture exist. "Culture" is the collective meaning a people put into their unique life-space. It is the pattern of attitudes, beliefs, customs, and traditions that generally expresses the way the average person in that place thinks and behaves.[3] Culture gives people a sense of who they are, of belonging, of how they should behave, and of what they should be doing. Culture is a distinctly human capacity for adapting to circumstances and transmitting this coping skill and knowledge to subsequent generations. Culture itself is an attempt, consciously or unconsciously, by a people to transmit to future generations their acquired wisdom and insight relative to their knowledge, beliefs, customs, traditions, morals, law, art, communication, and habits.

As mentioned earlier, culture provides a people with identity. Harris and Moran summarized characteristics of culture into 10 categories:

1. Sense of self and space
2. Communication and language
3. Dress and appearance
4. Food and feeding habits
5. Time consciousness
6. Relationships
7. Values and norms
8. Beliefs and attitudes
9. Mental process and learning
10. Work habits and practices

Corporate culture affects how an organization copes with competition and change, whether in terms of technology, economics, or people. The work culture stimulates or constricts the

[3] Philip R. Harris and Robert T. Moran, *Managing Cultural Differences*, 3rd ed. (Houston: Gulf Publishing, 1991).

energies of personnel, whether through slogans and myths or taboos. Today management is more cognizant of its customs and traditions, rules and regulations, policies and procedures—such components of culture are being used to make work more enjoyable, to increase productivity, and to meet customer needs and competitive challenges.

(i) Effects of Cultures

Persons of dissimilar backgrounds usually require more time than those of the same culture to become familiar with each other, be willing to speak openly, share sufficiently in common ideas, and understand one another.

Therefore, education and training of global leaders must include formal learning in the various cultural dimensions. With the globalization of business, managers and leaders need to become more transnational and transcultural in their thinking, planning, and involvement with people.

Culture also affects high-technology exporters and their share of the world market. For example, European firms view technological innovation as a danger with problems rather than an opportunity whereas the Americans and Japanese intuitively see the benefits of new technology. Unless such cultural handicaps are countered, Europe may not be able to take full advantage of some emerging markets.

Differences in customs, behavior, and values result in problems that can be managed only through effective cross-cultural communication and interaction. When people have misunderstandings or commit "errors" when working with persons from different cultures, they are often unaware of any problem. Cross-cultural mistakes result when we fail to recognize that persons of other cultural backgrounds have different goals, customs, thought patterns, and values from our own. Differences do not necessarily mean barriers; they can become bridges to understanding and enrichment of human lives.

(ii) Global Manager's Dilemma

Global managers operating transnationally are commonly faced with the following situation: In one country something is a lawful or accepted practice, and elsewhere it is illegal. Bribes, for example, may be a common way of doing business to ensure service in the host-country culture but quite illegal in the home-country culture.

Advances in mass media, transportation, and travel are breaking down the traditional barriers among groups of peoples and their differing cultures, so that a homogenization process is under way. Global managers should be alert to serving this new community in human needs and markets with strategies that are transnational.

Global planning requires not only an effective international management information system but input from a variety of locals at different levels of sophistication. Even when there are apparent similarities of people in geographic regions, cultural differences may require alteration of strategic market planning. For example, North American companies and unions discovered this in Canada when they tried to treat their operations in Canada as mere U.S. extensions. Europeans realized this in Bolivia and Argentina where political and social conditions altered a common cultural heritage.

(iii) Regional Cultures

Even in the United States, there are cultural differences between the South and the North and between the East and the West. Food habits, language, accent, pace of life, work attitudes, and values are different.

Culture affects decision making too. Robert Doktor,[4] a professor at the University of Hawaii, contrasted Japanese chief executive officers (CEOs) with their American counterparts and discovered significant differences in the way each group thinks and solves problems. The Japanese interviewed, for instance, spent most of their time with their people—they tended to engage in fewer work activities, but for a longer duration than their Western colleagues. Doktor concluded that Japanese CEOs go about problem solving in a more planned and orderly manner indicative of left-hemisphere dominance, fulfilling their role in ways quite opposite from what other researchers discovered about American executives.

(iv) Global Communication Insights

All behavior is communication because all behavior contains a message, whether intended or not. Communication is not static and passive; rather it is a continuous and active process without beginning or end. A communicator is not simply a sender or a receiver of messages but can be both at the same time. Culture poses communication problems because there are so many variables unknown to the communicators. *As the cultural variables and differences increase, the number of communication misunderstandings increases.*

Let us look at few examples of communication insights in a global context.

- The American manager who gives a gift of yellow flowers in France or white flowers in Japan has communicated something but probably not that which was intended. In France, yellow flowers suggest infidelity; white flowers are given at funerals in Japan to indicate sympathy.
- The American manager who has sharply disagreed with a Saudi Arabian in the presence of others has committed an "impoliteness" in the Arab world that is difficult to remedy.
- During an evening meal, a business conversation with a French manager in France may be very inappropriate.
- Space is also a factor in the communication process. The United States is a noncontact society and requires distance between people during a conversation. Many cultures, such as Latin American and Middle Eastern, are contact societies and require relatively close physical proximity to others during a conversation. Between males, touching is common and handshakes are frequent and last throughout a litany of greetings.
- Most persons use their hands when speaking to punctuate the flow of conversation, refer to objects or persons, and mimic or illustrate words or ideas. Often gestures are used in place of words. Generally, Japanese speakers use fewer words and fewer gestures than American speakers; French use more of both, and Italians much more.

(v) High- and Low-Context Communications

Anthropologist Edward Hall[5] makes a vital distinction between high- and low-context cultures and how the matter of context impacts communications. A high-context culture uses high-context communications—that is, information is either in the physical context or internalized in the person. Japan, Saudi Arabia, and Africa are examples of cultures engaged in high-context communications, as are the Chinese and Spanish languages. However, a low-context culture

[4] Ibid. Robert Doktor was mentioned in this book without any specific reference to Doktor.
[5] E. T. Hall and M. R. Hall, *Understanding Cultural Differences: Keys to Success in West Germany, France, and the United States* (Yarmouth, ME: Intercultural Press), 1990.

employs low-context communications—most information is contained in explicit codes, such as words. North American cultures engage in low-context communications, whether in Canada or the United States, and English is a low-context language.

In the communication process, a low-context culture places meaning in the exact verbal description of an event. Individuals in such a culture rely on the spoken word. The common statement that typifies this idea is "Say what you mean." However, in the high-context culture, much of the meaning is not from the words but is internalized in the person. Meaning comes from the environment and is looked for in the relationships between the ideas expressed in the communication process. *High-context cultures tend to be more human-oriented than low-context cultures. The extended family concept fits into the high-context culture.*

During negotiations or when working with Japanese and Latin Americans, they are looking for meaning and understanding in what is not said—in the nonverbal communication or body language, in the silences and pauses, in relationships and empathy. North Americans place emphasis on sending and receiving accurate messages directly, usually by being articulate with words. Specifically, Japanese communicate by not stating things directly, while Americans usually do just the opposite and spell it all out.

(vi) General Characteristics of the Emerging Work Culture

Harris's research[6] identified 10 general characteristics of the emerging work culture. Workers at all levels in the future will generally manifest or seek more

1. Enhanced quality of work life.
2. Autonomy and control over their work space.
3. Organizational communication and information orientation.
4. Participation and involvement in the enterprise.
5. Creative organizational norms or standards.
6. High performance and improved productivity.
7. Emphasis on new technology utilization.
8. Emphasis on R&D.
9. Emphasis on entrepreneurialism.
10. Informal and synergistic relationships.

(vii) Cultural Awareness Learning Program

The aim of the Canadian International Development Agency's training program is to instill seven skills that could be offered as the objectives of all cultural awareness learning. These skills can be applied to understand people, whether they are local, regional, or international. These skills are listed next.

1. **Communicate respect** to transmit (both verbally and nonverbally) positive regard, encouragement, and sincere interest.

[6] Ibid.

2. **Be nonjudgmental** to avoid moralistic, value-laden, evaluative statements and to listen in such a way that the other can fully share and explain itself.
3. **Personalize knowledge and perceptions** to recognize the influence of one's own values, perceptions, opinions, and knowledge on human interaction and to regard such as relative, rather than absolute, for more tentative communications.
4. **Display empathy** to try to understand others from their point of view, attempt to put oneself into the other's life space, and feel as they do about the matter under consideration.
5. **Practice role flexibility** to be able to get a task accomplished in a manner and time frame appropriate to the learner or other national and be flexible in the process for getting jobs done, particularly with reference to participation and group maintenance or morale.
6. **Demonstrate reciprocal concern** to truly open up a dialogue, take turns talking, share the interaction responsibility, between groups, and promote circular communication.
7. **Tolerate ambiguity** to be able to cope with cultural differences, try to accept a degree of frustration, and deal with changed circumstances and people.

These seven skills are associated with effective managing and transferring knowledge in a different culture. The degree to which managers and auditors possess these skills marks their potential effectiveness in working in a multicultural environment.

(b) Cross-Cultural Negotiations

Negotiating across cultures is far more complex than negotiating within a culture because foreign negotiators have to deal with differing negotiating styles and cultural variables simultaneously. In other words, the negotiating styles that work at home generally do not work in other cultures. As a result, cross-cultural business negotiators have one of the most complicated business roles to play in organizations. They are often thrust into a foreign society consisting of what appears to be hostile strangers. They are put in the position of negotiating profitable business relationships with these people or suffering the negative consequences of failure. And quite often they find themselves at a loss as to why their best efforts and intentions have failed them.

(i) How to Avoid Failure in International Negotiations

Negotiators in a foreign country often fail because local counterparts have taken more time to learn how to overcome the obstacles normally associated with international/cross-cultural negotiations. Failure may occur because of time and/or cost constraints. For example, a negotiator may be given to a short period of time to obtain better contract terms than were originally agreed to in a country where negotiations typically take a long time. A negotiator may think what works in the home country is good enough for the rest of the world, but it is far from the truth. In fact, strategies that fail to take into account cultural factors are usually naive or misconceived. Typically, the obstacles to overcome include

- **Learning the local language**, or at least being able to select and use an effective language translator.
- **Learning the local culture**, including how the culture handles conflict, its business practices, and its business ethics, or at least being able to select and use an effective cultural translator.
- **Arriving well prepared for the negotiations.** Along with the prior points, the negotiator must have a thorough knowledge of the subject matter being negotiated.

Effective cross-cultural negotiators understand the cultural differences existing among all parties involved, and they know that failure to understand the differences serves only to destroy potential business success.

(ii) How Much Must One Know about the Foreign Culture?

Realistically, it is nearly impossible to learn everything about another culture, although it may be possible if one lives in the culture for several years. The reason for this is that each culture has developed, over time, multifaceted structures that are much too complex for any foreigner to understand totally. Therefore, foreign negotiators need not have total awareness of the foreign culture; they do not need to know as much about the foreign culture as the locals, whose frames of reference were shaped by that culture. However, they will need to know enough about the culture and about the locals' negotiating styles to avoid being uncomfortable during (and after) negotiations. Besides knowing enough to not fail, they also need to know enough to win. For example, in negotiations between Japanese and American businesspeople, Japanese negotiators have sometimes used to their advantage their knowledge that Americans have a low tolerance for silence.

In other words, in order for negotiation to take place, foreigners must at least recognize those ideas and behaviors that the locals intentionally put forward as part of the negotiation process—and the locals must do the same for the foreigners. Both sides must be capable of interpreting these behaviors sufficiently to distinguish common from conflicting positions, spot movement from positions, and respond in ways that sustain communication. Ultimately, cross-cultural negotiators must determine their counterparts' personal motivations and agendas and adapt the negotiation style to them.

The purpose of the previous discussion is to develop a cross-cultural negotiating process. The process includes both strategy and tactics. **Strategy** refers to a long-term plan, and **tactics** refers to the actual means used to implement the strategy.

(iii) Strategic Planning for International Negotiations

Strategic planning for international negotiations involves five stages:

1. Preparation for face-to-face negotiations
2. Determining the settlement range
3. Determining where the negotiations should take place
4. Deciding whether to use an individual or a group of individuals in the negotiations
5. Learning about the country's views on agreements/contracts

Tactical planning for international negotiations involves determining how to obtain leverage, use delay tactics, and deal with emotions.

(iv) Ethical Constraints

Business ethics and corporate social responsibility place constraints on negotiators. For example, a negotiator's ethical concerns for honesty and fair dealings, regardless of the power status of negotiating parties, will affect the outcome. There is no global standard or view of what is ethical or unethical behavior in business transactions—what is viewed as unethical behavior in one

culture may be viewed as ethical in another culture, and vice versa. For instance, if a negotiator on one side pays off an influential decision maker on the other side to obtain a favorable decision, it would be an unethical business practice in some cultures (and illegal in the United States), but it would be quite acceptable in other cultures.

(v) International Management Theories

Theory Z, coined by William Ouichi,[7] refers to a Japanese style of management that is characterized by long-term employment, slow promotions, considerable job rotation, consensus-style decision making, and concern for the employee as a whole.

Theory T and **Theory T+** are complementary theories based on these Southeast Asian assumptions:

- Work is a necessity but not a goal itself.
- People should find their rightful place in peace and harmony with their environment.
- Absolute objectives exist only with God.
- In the world, persons in authority positions represent God, so their objectives should be followed.
- People behave as members of a family and/or group, and those who do not are rejected by society.

(c) Global Mindsets

Cultural forces represent another important concern affecting international human resources (HR) management. In addition to organizational culture, national cultures also exist. **Culture** is composed of the societal forces affecting the values, beliefs, and actions of a distinct group of people. Cultural differences certainly exist between nations, but significant cultural differences exist within countries also. One only has to look at the conflicts caused by religion or ethnicity in Central Europe and other parts of the world to see the importance of culture in international organizations. Convincing individuals from different ethnic or tribal backgrounds to work together may be difficult in some parts of the world.

Geert Hofstede[8] conducted research on more than 100,000 IBM employees in 53 countries, and he defined these five dimensions useful in identifying and comparing culture:

1. Power distance
2. Individualism
3. Masculinity/femininity
4. Uncertainty avoidance
5. Long-term orientation

[7] W. G. Ouichi and A.M. Jaeger, "Made in America under Japanese Management," *Harvard Business Review* (September–October 1974).
[8] Geert Hofstede, *Cultural Consequences: International Differences in Work-Related Values* (Beverly Hills, CA: Sage, 1984).

The dimension of **power distance** refers to the inequality among the people of a nation. In countries such as Canada, the Netherlands, and the United States, there is less inequality than in such countries as France, Mexico, and Brazil. As power distance scores increase, there is less status and authority difference between superiors and subordinates.

One way in which differences on this dimension affect HR activities is that the reactions to management authority differ among cultures. A more autocratic approach to managing is more common in many countries, while in the Netherlands and the United States, there may be more use of employee participation in decision making.

Another dimension of culture identified by Hofstede is **individualism**, which is the extent to which people in a country prefer to act as individuals instead of members of groups. On this dimension, people in some Asian countries tend to be less individualistic and more group oriented, whereas those in the United States are more individualistic. An implication of these differences is that more collective action and less individual competition are likely in those countries that deemphasize individualism.

The cultural dimension **masculinity/femininity** refers to the degree to which "masculine" values prevail over "feminine" values. Masculine values identified by Hofstede were assertiveness, performance orientation, success, and competitiveness; feminine values included quality of life, close personal relationships, and caring. Respondents from Japan had the most masculinity, while those from the Netherlands had more femininity-oriented values. Differences on this dimension may be tied to the role of women in the culture. Considering the different roles of women and what is "acceptable" for women in the United States, Saudi Arabia, Japan, and Mexico suggests how this dimension might affect the assignment of women expatriates to managerial jobs in the various countries.

The dimension of **uncertainty avoidance** refers to the preference of people in a country for structured rather than unstructured situations. A structured situation is one in which rules can be established and there are clear guides on how people are expected to act. Nations focusing on avoiding uncertainty, such as Japan and France, tend to be more resistant to change. In contrast, people in places such as the United States and Great Britain tend to have more "business energy" and to be more flexible.

A logical use of differences in this factor is to anticipate how people in different countries will react to changes instituted in organizations. In more flexible cultures, what is less certain may be more intriguing and challenging, which may lead to greater entrepreneurship and risk taking than in the more "rigid" countries.

The dimension of **long-term orientation** refers to values people hold that emphasize the future, as opposed to short-term values, which focus on the present and the past. Long-term values include thrift and persistence, while short-term values include respecting tradition and fulfilling social obligations. Hofstede developed this dimension a decade after his original studies on dimension. A long-term orientation was more present in Japan and India, while people in the United States and France tended to have more short-term orientations.

Differences in many other facets of culture could be discussed. But it is enough to understand that international HR managers and professionals must recognize that cultural dimensions differ from country to country and even within countries. Therefore, the HR activities appropriate in one culture or country may have to be altered to fit appropriately into another culture or country.

8.3 Legal and Economic Concepts

Topics such as contracts and key economic indicators are discussed in this section.

(a) Contracts

(i) Definition of a Contract

Contracts are governed by state common law. A contract is a binding agreement that the courts will enforce. It is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes a duty. A promise manifests or demonstrates the intention to act or to refrain from acting in a specified manner.

Those promises that meet all of the essential requirements of a binding contract are contractual and will be enforced. All other promises are not contractual, and usually no legal remedy is available for a breach of, or a failure to properly perform, these promises. The remedies provided for breach of contract include compensatory damages, equitable remedies, reliance damage, and restitution. Thus, a promise may be contractual (and therefore binding) or noncontractual. In other words, all contracts are promises, but not all promises are contracts.

(ii) Requirements of a Contract

The four basic requirements of a contract include (1) mutual assent, (2) consideration, (3) legality of object and subject matter, and (4) capacity (competent parties).

- **Mutual assent.** The parties to a contract must manifest by words or conduct that they have agreed to enter into a contract. The usual method of showing mutual assent is by offer and acceptance. An offer is a proposal or expression by one person that he is willing to do something for certain terms. A contract does not exist until the offer is formally accepted, either verbally or in written form. The offer and acceptance have to match. If they match, there is an agreement leading up to a contract. If they do not, it is more like a negotiation, to which someone responds with a counteroffer rather than an acceptance, which continues until both parties reach an agreement, or a meeting of the minds.
- **Consideration.** Each party to a contract must intentionally exchange a legal benefit or incur a legal detriment as in inducement to the other party to make a return exchange. Consideration is a form of "mutual obligation." In the business world, mutual promises in a contract of sale, whether express or implied, are generally sufficient consideration.
- **Legality of object and subject matter.** The purpose of a contract must not be criminal, tortious, or otherwise against public policy. If the purpose is illegal, the resulting contract is null and void. The performance of a party in regard to the contract must not be an unlawful act if the agreement is to be enforceable. However, if the primary purpose of a contract is legal, but some terms contained within the agreement are not, then the contract may or may not be itself be illegal, depending on the seriousness of the illegal terms and the degree to which the legal and illegal terms can be separated.
- **Capacity (competent parties).** The parties to a contract must have contractual capacity. Certain persons, such as adjudicated incompetents, have no legal capacity to contract, while others, such as minors, incompetent persons, and intoxicated persons, have limited capacity to contract. All others have full contractual capacity. The parties can be principals or qualified agents. The parties cannot engage in any fraudulent activities. The use of force

or coercion to reach an agreement is not acceptable in signing a contract because both parties must enter into the agreement on their own free will. Both parties must indicate a willingness to enter into the agreement and be bound by its terms.

In addition, although in a limited number of instances a contract must be evidenced in writing to be enforceable, in most cases an oral contract is binding and enforceable. Moreover, there must be an absence of invalidating conduct, such as duress, undue influence, misrepresentation, or mistake. A promise meeting all of these requirements is contractual and legally binding. However, if any requirement is unmet, the promise is noncontractual.

(iii) Classification of Contracts

Contracts can be classified according to various characteristics, such as method of formation, content, and legal effect. The standard classifications are listed next.

- Express or implied contracts
- Bilateral or unilateral contracts
- Valid, void, voidable, or unenforceable contracts
- Executed or executory contracts

These classifications are not mutually exclusive. For example, a contract may be express, bilateral, valid, executory, and informal.

- **Express and implied contracts.** A contract formed by conduct is an implied or, more precisely, an implied-in-fact contract. In contrast, a contract in which the parties manifest assent in words is an express contract. Both are contracts, equally enforceable. The difference between them is merely the manner in which the parties manifest their assent.
- **Bilateral and unilateral contracts.** When each party is both a promisor (a person making a promise) and a promisee (the person to whom a promise is made), it is called a bilateral contract. A unilateral contract is one where only one of the parties makes a promise.
- **Valid, void, voidable, and unenforceable contracts.** A valid contract is one that meets all of the requirements of a binding contract. It is an enforceable promise or an agreement. A void contract is an agreement that does not meet all of the requirements of a binding contract. It has no legal effect and is merely a promise or agreement. An example is an agreement entered by a person whom the courts have declared incompetent. A contract that is neither void nor voidable may nonetheless be unenforceable. An unenforceable contract is one for the breach of which the law provides no remedy. After the statutory time period has passed, a contract is referred to as unenforceable rather than void or voidable.
- **Executed and executory contracts.** A contract that has been fully carried out and completed by all of the parties to it is an executed contract. By comparison, the term "executory contract" applies to contracts that are still partially or entirely unperformed by one or more of the parties.

(iv) Other Types of Contracts

Two other types of contracts that occur in common include the doctrine of promissory estoppel and quasi contracts.

(A) Doctrine of Promissory Estoppel In certain circumstances, the courts enforce noncontractual promises under the doctrine of promissory estoppel in order to avoid injustice. A noncontractual promise is enforceable when it is made under circumstances that should lead the promisor reasonably expect that the promisee, in reliance on the promise, would be induced by it to take definite and substantial action or to forbear, and the promisee does take such action or does forbear.

(B) Quasi Contracts A quasi (meaning "as if") contract is not a contract at all. A quasi contract is based on neither an express nor an implied in fact contract. Rather, a quasi contract is a contract implied in law, which is an obligation imposed by law to avoid injustice. Occasionally quasi contracts are used to provide a remedy when the parties enter into a void contract, an unenforceable contract, or a voidable contract that is avoided. In such a case, the law of quasi contracts will determine what recovery is permitted for any performance rendered by the parties under the invalid, unenforceable, or invalidated agreements.

(b) Key Economic Indicators

(i) Nature of Key Economic Indicators

Business conditions relate to business cycles. Decisions such as ordering inventory, borrowing money, increasing staff, and spending capital are dependent on the current and predicted business cycle. For example, decision making in preparation for a recession, such as cost reduction and cost containment, is especially different and difficult. Also, during a recession, defaults on loans can increase due to bankruptcies and unemployment.

Timing is everything when it comes to making good cycle-sensitive decisions. Managers need to make appropriate cutbacks prior to the beginning of a recession. Similarly, managers cannot get caught short during a period of rapid expansion. Economic forecasting is a necessity for predicting business cycles and swings. Trend analysis, economic surveys, opinions, and simulation techniques are useful to managers trying to stay abreast of the latest economic developments.

Businesses use economic forecasts in making investment and production decisions. When they foresee an economic downturn, inventories may be reduced. When prices are expected to rise quickly, they buy goods in advance and add to equipment and plant.

Statistical models are most successful when past circumstances can be used to predict future events. Economic models use historical data to develop predictive models. Current input to the model provides a meaningful production only if the important factors retain the same proportional significance. During the energy crisis of the early 1970s, most economic models performed very poorly because key relationships had changed. Thus, predictive models improved once new historical patterns emerged.

The opposite of forecasting economic events is measuring economic events. This historical information is important in evaluating and providing information for predicting the future. The business cycle is the up-and-down movement of an economy's ability to generate wealth. Historical economic data show a clear pattern of alternating recessions and expansions. In between there have been peaks and troughs of varying magnitude and duration. Business cycles have a predictable structure but variable timing.

(ii) Specific Types of Key Economic Indicators

Three types of economic indicators are used in forecasting, including leading indicators, coincident indicators, and lagging indicators (see Exhibit 8.4).

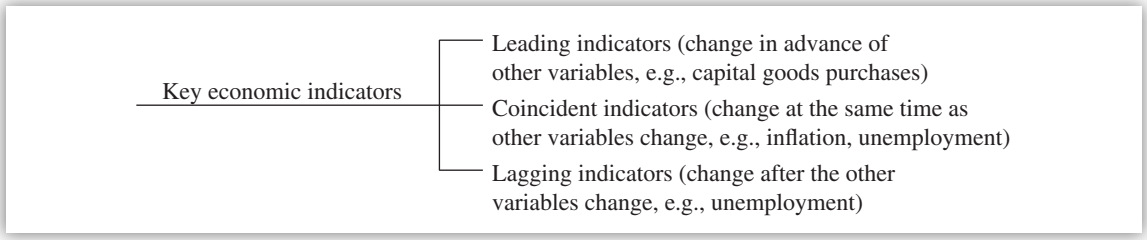


EXHIBIT 8.4 Key Economic Indicators

1. **Leading indicators** change in advance of other variables. These are the least likely to be accurate. However, they are the most useful for business planning, because they provide information for action. Example: Capital goods purchases are a leading indicator for recession. The Consumer Price Index is often used in making plans for inflation and wages because it is a leading economic indicator.
2. **Coincident indicators** change at the same time as other variables change. Example: Inflation, unemployment, and consumer confidence are coincident indicators.
3. **Lagging indicators** change after the other variables change. These are more accurate, but the information is much less useful for decision making. Example: Unemployment figures are lagging indicators of recession.

(iii) Other Types of Key Economic Indicators

Other types of key economic indicators include gross national product (GNP), gross domestic product (GDP), net national product (NNP), consumer price index (CPI), and producer price index (PPI). These are discussed below.

(A) Gross National Product and Gross Domestic Product A measure of the change in prices for all final goods and services produced in the economy is the GNP price deflator. This inflation index can be used to estimate the inflation rate on all goods and services over a recent time period.

The following list provides relationships among GNP, GDP, NNP, CPI, and PPI.

- The two main variables that contribute to increases in a nation's real GDP are labor productivity and total worker hours.
- NNP is composed of the total market value of all final goods and services produced in the economy in one year minus the capital consumption allowance.
- The basic source of improvements in real wage rates and in the standard of living is productivity growth.
- Under the income approach, GNP is measured as follows: Depreciation charges + Indirect business taxes + Wages, rents, interest, and profits.
- In the output (expenditures) approach to measuring a country's GNP, it is calculated as follows: Consumption + Investments + Government purchases + Expenditures by foreigners.

- When gross investment is less than depreciation, the capital stock of the economy is shrinking.
- An increase in the average hours worked per week of production workers would provide a leading indicator of a future increase in GNP.
- The sale of final goods is included in the GNP, and the sale of intermediate goods is excluded from the GNP.
- GNP price deflator is the price index for all final goods and services used to adjust the money (or nominal) GNP to measure the real GNP.

(B) Consumer Price Index and Producer Price Index CPI is a statistic used to measure the changes in prices in a market basket of selected items. CPI is one factor in setting cost of living adjustments in a country. Critics of CPI argue that it overstates increases in the cost of living. This is due to the constant composition of the market basket of items whose prices are measured. The PPI measures the price of a basket of commodities at the point of their first commercial sale.

Example: Application of CPI, Real Income, and Inflation

Assume that in 1990, an internal auditor is making $40,000 per year. Five years later, his income has risen to $90,000, but the CPI has increased from 100 to 250. The real income (in 1990 prices) for the later year is calculated as follows:

The inflation rate is (250 – 100)/250 = 150/250 = 0.60, that is, 60%.

Real income is nominal income minus inflation rate, that is, 100% – 60% = 40%.

Therefore, real income is $90,000 × 0.40 = $36,000.

(iv) Methods of Measuring Economic Performance

The basic goals of the public and private sectors are to achieve both the full employment of resources and a stable price level. *Two major methods exist to measure economic performance of a country: unemployment and inflation.*

(A) Unemployment The key point is that the level of output depends directly on total or aggregate expenditures. A high level of total spending means that it will be profitable for the various industries to produce large outputs, and it will be profitable for various resource suppliers to be employed at high levels. Hence,

Total spending = Private sector spending + Public sector spending

Private sector spending alone is not enough to keep the economy at full employment. The government's obligation (public spending) is to augment private sector spending sufficient enough to generate full employment. *Government has two basic economic tools with which to accomplish public spending: spending programs and taxes.* Specifically, government should increase its own spending on public goods and services on one hand and reduce taxes in order to stimulate private sector spending on the other. Unemployment results when either private sector spending or public sector spending does not measure up to expectations.

There are four variations of unemployment: (1) full employment, (2) frictional unemployment, (3) cyclical employment, and (4) structural unemployment (see Exhibit 8.5).

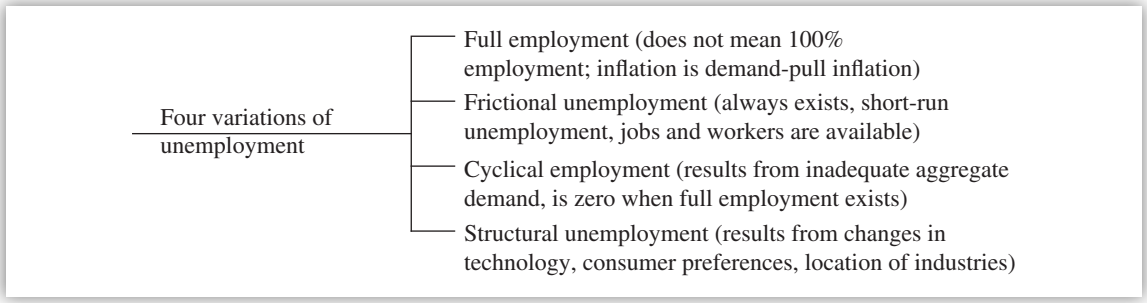


EXHIBIT 8.5 Four Variations of Unemployment

Full employment means that all people 16 years of age or older are employed or are actively seeking employment or that cyclical unemployment is zero. Inflation occurring during a period of full employment is most likely to be a demand-pull inflation. In an economy that is near full employment, a decrease in the money supply is likely to decrease the price level.

TYPES OF EMPLOYMENT/UNEMPLOYMENT

- Full employment means that all people available to produce goods and services are employed.
- Frictional unemployment is short run and caused by people voluntarily changing jobs.
- Cyclical employment results from inadequate aggregate demand.
- Structural unemployment results from an economy's failure to adjust to changes in technology, consumer preferences, or locations of industries.

Frictional unemployment will always exist in a dynamic economy. It is short-run unemployment that is caused by people voluntarily changing jobs or by frictions that result from lack of knowledge about job opportunities and lack of labor mobility.

Thus, full employment means that only frictional unemployment exists. In other words, there is no cyclical or structural unemployment when the economy is operating at full employment. There always will be some unemployment caused by workers changing jobs. Frictional unemployment occurs when both jobs and the workers qualified to fill them are available. It is equal to about 5% or 6%.

Cyclical employment is unemployment that results from inadequate aggregate demand during the recession and depression phases of the business cycle.

Structural unemployment is unemployment that results from an economy's failure to adjust completely and efficiently to basic structural changes, such as changes in technology, changes in consumer preferences, and changes in the geographical locations of certain industries. It is equal to about 5% or 6%.

Structural changes prevent certain people from obtaining jobs because of their geographical location, race, age, inadequate education, or lack of training. *People who are structurally unemployed often are referred to as the hard-core unemployed.*

(B) Inflation and Deflation If aggregate spending exceeds the full-employment output, the excess spending will have the effect of increasing the general price level. Therefore, excessive aggregate spending is inflationary. Government intervenes to eliminate the excess spending by cutting its own expenditures and by raising taxes so as to curtail private spending. The inverse relationship between unemployment and inflation is embodied in the Phillips curve.

UNEMPLOYMENT AND INFLATION DILEMMA

- Total spending should increase to generate full employment.
- Excessive aggregate spending leads to inflation.
- An increase in the price level would tend to decrease consumption.

Inflation is a rise in the general level of prices; deflation is a decline in the general level of prices. However, inflation has been the prevailing condition in the United States in recent decades.

When prices rise, purchasing power, or the ability to buy goods and services, declines. If prices double, purchasing power is reduced to one-half of its previous level. Thus, *inflation reduces the purchasing power of money.* Inflation does not mean that the prices of all goods and services rise. Some prices rise, others fall, and some do not change at all, but, on the average, prices rise.

The basic cause of inflation is spending in excess of what an economy can produce. If an economy has unemployed resources, an increase in aggregate demand tends to increase output and employment a great deal and to increase prices only slightly. When an economy is fully employed, an increase in aggregate demand forces prices to increase sharply because resources are scarce and output cannot be increased.

(v) Types of Inflation

In reality, there are seven types of inflation, which are presented below (see Exhibit 8.6).

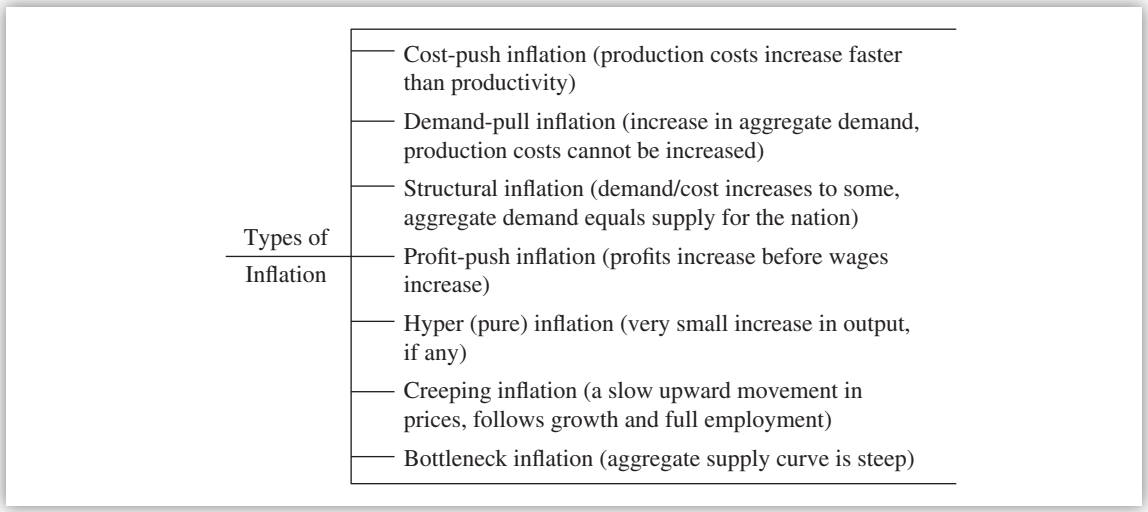


EXHIBIT 8.6 Seven Types of Inflation

1. **Cost-push inflation** is a rise in prices brought about by production costs increasing faster than productivity. Since labor is usually the largest cost of production, cost-push inflation is often called wage-push inflation. The expected impact is an increase in unemployment.
2. **Demand-pull inflation** is a rise in prices that is caused by an increase in aggregate demand when an economy's resources are fully employed and production cannot be increased. The expected impact is a decrease in unemployment.
3. **Structural inflation** results when demand increases or costs increase in certain industries even though aggregate demand equals aggregate supply for the nation as a whole.

TYPES OF INFLATION

- Cost-push inflation is caused by increase in wages and prices.
- Demand-pull inflation is caused by increase in aggregate demand.
- Structural inflation results when demand increases or cost increases in certain industries.
- Profit-push inflation occurs when corporate profits increase before wages increase.
- Hyperinflation or pure inflation is a rise in prices with a very small increase in output.
- Creeping inflation is a slow upward movement in prices over a period of several years.
- Bottleneck inflation occurs when the aggregate supply curve is steep.

4. **Profit-push inflation** occurs when corporate profits increase before wages increase. An increase in corporate profits can result from increases in prices or from improvements in productivity that reduce the labor cost per unit.
5. **Hyperinflation or pure inflation** is a rise in prices with a very small, if any, increase in output.
6. **Creeping inflation** is a slow upward movement in prices over a period of several years. Creeping inflation is usually defined as a 1%, 2%, or 3% increase in the general price level each year. Creeping inflation generally accompanies growth and full employment. Many economists prefer creeping inflation to price stability accompanied by unemployment and lack of economic growth.
7. **Bottleneck inflation** can be associated with an aggregate supply curve that is steep.

Before the redistribution effects of inflation can be discussed, a distinction must be made between money income and real income. **Money income** is the amount of money or number of dollars a person receives for the work he or she does; real income is the amount of goods and services the money income will buy or the purchasing power of the money income. **Real income** is thus a function of money income and the prices of goods and services.

(vi) Effects of Inflation

If nominal income increases faster than the price level, then real income will rise. Three classes of people generally suffer from inflation, and three classes of people generally benefit from inflation.

1. **Those who suffer are fixed money income groups, creditors, and savers.** People who have **fixed money incomes**, or incomes that rise slower than prices, suffer from

inflation because their real income declines when prices increase faster than their money incomes increase. Unanticipated inflation will always adversely affect the wealth of lenders with fixed rate mortgage loans. Low-fixed-income individuals with no debts would likely suffer most adversely from inflation. Inflation reduces the value of a fixed income.

VARIABLE INCOME VERSUS FIXED INCOME

- Individuals with variable incomes and debts gain from inflation by paying them with dollars of lesser value than the amounts originally borrowed.
- Individuals with low fixed income with no debts do not have the advantage enjoyed by middle- to upper-middle-class and rich individuals.

Creditors suffer from inflation because the loans they make are paid back with dollars of less purchasing power than the dollars they lent. **Savers** suffer just like creditors, since the money people save declines in purchasing power as prices rise.

2. **Those who benefit are flexible money income groups, debtors, and speculators. Flexible money income groups**, or people whose incomes rise faster than prices rise, benefit from inflation because they experience an increase in their real incomes. **Debtors** benefit because they pay off their loans with dollars that are "cheaper" (worth less) than the dollars they borrowed. **Speculators**—people who buy goods in anticipation of making profits when prices change—can increase their real wealth if they borrow money to buy goods during inflation.

It is interesting to note that inflation redistributes wealth and income unevenly by penalizing some groups and bestowing benefits on other groups (assuming full employment). Inflation is often called the cruelest tax because it penalizes those who are the most vulnerable to it. A higher inflation rate generally results in higher nominal interest rates.

(vii) Nature of Deflation

Deflation is a decrease in prices. Deflation can be induced through contractionary monetary and fiscal policies. If deflation occurs in the United States, it becomes cheaper for other countries to buy U.S. goods. Deflation can arise automatically due to an excess of imports over exports.

8.4 Impact of Government Legislation and Regulation on Business

Topics such as governmental legislation and regulation, government's monitoring of environmental issues, specific trade legislation, and regulations such as tied aid practices and the U.S. Export-Import bank, and international laws such as World Trade Organization (WTO), North American Free Trade Agreement (NAFTA), and the European Union (EU) are discussed in this section.

Government impacts business in many ways. This impact is felt through regulations to control environment, labor practices, safety at workplace, product liability, import and export laws,

banking practices, and other areas. Government also impacts business through depreciation laws and tax credits to control investment levels in the economy by the private sector. Using fiscal and monetary policies, government controls employment, production, inflation, interest rates, government spending, and money supply in the economy.

For example, the Consumer Product Safety Commission enforces the Consumer Product Safety Act, which covers safety of any consumer product not addressed by other regulatory agencies. The Food and Drug Administration enforces laws and develops regulations to prevent distribution and sale of adulterated foods, drugs, cosmetics, and hazardous consumer products. The manufacturer is usually liable for dangerous and unsafe products. Government laws and regulations can appear as a constraint on business behavior. Another way to view them is as an opportunity to provide safer and more efficient products to consumers. Events such as deregulation in the airlines and telecommunications industries have helped both producers and consumers alike.

(a) Governmental Legislation and Regulation

Governmental legislation and regulation includes both state and federal government. The scope of state regulation includes pricing by public utility companies while the scope of federal regulation covers price fixing, deceptive pricing, price discrimination, and promotional pricing. Examples include:

- Sherman Antitrust Act
- Clayton Act
- Federal Trade Commission Act
- Robinson-Patman Act
- Wheeler-Lea Act
- Celler Antimerger Act

These federal statutes when combined with state legislation intend to promote and preserve competition in a free enterprise system and to prevent monopoly power. These acts cover interstate commerce among the several states but not intrastate activity. All states have antitrust statutes applicable to intrastate activity.

(i) Sherman Act

The Sherman Act of 1880 is the primary, first tool of antitrust enforcement. The act declared illegal any combination, contract, or conspiracy in restraint of trade made among the states or with foreign countries. The act also made it illegal to monopolize, attempt to monopolize, or conspire to monopolize any portion of interstate commerce or any portion of trade with foreign nations. However, the Sherman Act did not state exactly what types of action were prohibited. Two substantial provisions as defined in Sections 1 and 2 of the act are described next.

Section 1 states: "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal."

Section 1 is concerned with contract, combination, and conspiracies in restraint of trade. Two or more persons working together (i.e., combination) to fix prices or divide market to achieve the

anticompetitive results, for example, constitute a violation of the act. Conspiracy is concerned with the conduct of an individual firm (e.g., predatory pricing) to create or maintain a monopoly.

Restraint of trade consists of horizontal and vertical types. **A horizontal restraint** is an agreement among competitors, such as manufacturers, retailers, or wholesalers. Examples of horizontal restraints include division of markets, price fixing, group boycotts, and exchange of market information. **A vertical restraint** is an agreement between persons standing in a buyer–seller relationship (a manufacturer and a retailer in the same line of products). Examples of vertical restraint include resale price maintenance, location, territory, and customer restrictions, tying arrangements, and exclusive dealing contracts.

Section 2 states: "Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony."

The wording of the act is too broad and general and leaves much discretion to federal courts for interpretation. These two sections complement each other in achieving the goal of preventing monopoly and anticompetitiveness. *The Sherman Act requires proof of actual and substantial anticompetitive effect.*

Labor unions, agricultural cooperatives, fisherman's organizations, and export trade associations enjoy limited **antitrust exemption**.

VIOLATIONS OF THE SHERMAN ACT

Violations of both Sections 1 and 2 are felonies punishable by imprisonment of up to three years and fines up to $100,000, or both, for individuals and fines up to $1 million for corporations. Civil actions are more common than criminal proceedings.

Approximately 75% of civil suits are settled through consent decrees (a compromise between the government and the defendant). The Sherman Act also contains the seldom-used forfeiture remedy, where the property may be seized.

Conduct that would violate the Sherman Act in the absence of union involvement is not immunized by the participation of the union. For example, a union may not band together with a nonlabor party, such as a contractor or manufacturer, to achieve a result forbidden by the antitrust laws.

(ii) Clayton Act

The Clayton Act of 1914 was designed to strengthen and clarify the provisions of the Sherman Act. It defines specifically what constitutes monopolistic or restrictive practices, whereas the Sherman Act does not.

The Clayton Act makes price discrimination illegal unless it can be justified because of differences in costs. The act prohibits the use of exclusive or tying contracts when their use "substantially lessens competition or tends to create a monopoly." Exclusive or tying contracts are contracts in which the seller agrees to sell a product to a buyer on the condition that the buyer will not purchase products from the seller's competitors. The Clayton Act also makes intercorporate stockholdings illegal if they tend to greatly reduce competition or to create a monopoly. In addition, the Clayton Act makes interlocking directorates (having the same individual on two or more board

of directors) illegal if the corporations are competitive and if at least one of the corporations is of a certain minimum size.

Four provisions (sections 2, 3, 7, and 8) that are of importance are listed next.

- Section 2 prohibits certain types of price discrimination.
- Section 3 prohibits certain sales made on condition that the buyer not deal with the seller's competitors.

VIOLATIONS OF THE CLAYTON ACT

No criminal sanctions are imposed for violations of the Clayton Act. Private remedies and legal and equitable relief are available. Legal relief is a private action for money damages.

In a private action, the plaintiff must ordinarily prove both the existence of an antitrust violation and damages resulting from that violation.

- Section 7 prohibits certain corporate mergers.
- Section 8 prohibits a person serving on the board of directors of two competing companies (an "interlocking directorate) if one or both companies are larger than a given size.

The goal of the Clayton Act is to curb anticompetitive practices in their incipiency. Under the act, simply showing a probable, rather than actual, anticompetitive effect would be enough cause for a violation of the act. This means that the Clayton Act is more sensitive to anticompetitive practices than the Sherman Act.

The scope of the Clayton Act in mergers includes both asset and stock acquisitions. The act now covers both mergers between actual competitors and vertical and conglomerate mergers having the requisite anticompetitive effect.

RULES OF MERGERS

- A horizontal merger is one between former competitors.
- A vertical merger occurs when a firm acquires a supplier or customer.
- If a business acquires a supplier, it is said to vertically integrate backward, or upstream.
- If a business acquires a customer, it is said to vertically integrate forward, or downstream.
- A conglomerate merger involves parties who were neither former competitors nor in the same supply chain.

(iii) Federal Trade Commission Act

Like the Clayton Act, the Federal Trade Commission Act was designed to prevent abuses and to sustain competition. The act declared as unlawful "unfair methods of competition in commerce."

The act also established the Federal Trade Commission (FTC) in 1914 and gave it the power and the resources to investigate unfair competitive practices. The act authorizes the FTC to issue

cease-and-desist orders prohibiting "unfair methods of competition" and "unfair or deceptive acts or practices." These orders provide injunctive relief by preventing or restraining unlawful conduct. *One of the goals of the FTC is to enforce antitrust laws and to protect consumers.*

VIOLATIONS OF THE FTC ACT

No criminal sanctions are imposed for violations of the FTC Act. Most FTC investigations are settled by a consent order procedure.

Although no criminal sanctions or private damage remedies are imposed for FTC act violations, a $10,000-per-day civil penalty is imposed for violating cease-and-desist orders.

The FTC has a dual role in prohibiting unfair methods of competition and anticompetitive practices. *The FTC Act supplements the Sherman and the Clayton Acts.* The FTC protects consumers who are injured by practices such as deceptive advertising or labeling without regard to any effect on competitors.

Although not explicitly empowered to do so, the FTC frequently enforces the Sherman Act indirectly and enjoins conduct beyond the reach of either the Sherman or Clayton Acts.

(iv) Robinson-Patman Act

In 1936, Congress passed the Robinson-Patman Act, which amends the Clayton Act to protect small competitors. It is often called the chain store act. The Robinson-Patman Act amends the price discrimination section of the Clayton Act. It was aimed at protecting independent retailers and wholesalers from "unfair discriminations" by large chain stores and mass distributors, which were supposedly obtaining large and unjustified price discounts because of their purchasing power and bargaining position.

Both the Department of Justice and the FTC can proceed against violators of the Robinson-Patman Act. The act prohibits price discrimination (where a seller charges one buyer more than another for the same product). It makes it unlawful for sellers to grant concessions to buyers unless concessions are granted to all buyers on terms that are proportionally equal. The act reaches the quantity discount, a major form of price discrimination.

The Robinson-Patman Act made it illegal:

- To discriminate by granting unjustified quantity discounts that greatly reduce competition or tend to create a monopoly among sellers or buyers.
- To pay brokerage fees if no broker is involved in a transaction.
- To grant or obtain larger discounts than those available to competitors who purchase the same goods in the same amounts.
- For sellers to grant concessions to buyers unless concessions are created to all buyers on terms that are proportionally equal.

The act applies only to sales, not to leases, agency/consignment arrangements, licenses, or refusals to deal (selling to one firm while refusing to deal with another). The scope of the Robinson-Patman Act applies to tangible personal property (commodities) and in the sale of services or intangibles, such as advertising.

VIOLATIONS OF THE ROBINSON-PATMAN ACT

To violate the statute, the discrimination in price must be "between different purchasers." A mere showing of different prices charged is enough to violate.

A mere showing that competing buyers were charged different prices is generally sufficient to establish a prima facie Robinson-Patman Act violation. Proof of a prima facie case of price discrimination does not necessarily result in a liability.

The seller may avoid the consequences of the discrimination by proving one of three defenses: (1) the "cost justification" defense, (2) the "meeting competition" defense, and (3) the "changing conditions." The burden of proving a defense is on the discriminating seller.

(v) Wheeler-Lea Act

In 1938, the Wheeler-Lea Act was passed as an amendment to the FTC Act. The Wheeler-Lea Act makes "unfair or deceptive acts or practices" in interstate commerce illegal; thus, it is designed to protect consumers rather than competitors. With the passage of this act, the FTC has the authority to prohibit false and misleading advertising and product misrepresentation.

(vi) Celler Antimerger Act

The Celler Antimerger Act of 1950 also amended the Clayton Act by making it illegal for a corporation to acquire the assets, as well as the stock, of a competing corporation if the effect is to greatly reduce competition or to tend to create a monopoly.

(b) Government's Monitoring of Environmental Issues

The U.S. Environmental Protection Agency (EPA) protects and enhances the environment today and for future generations to the fullest extent possible under the laws enacted by the U.S. Congress. The agency's mission is to control and abate pollution in the areas of air, water, solid waste, pesticides, radiation, and toxic substances. Its mandate is to mount an integrated, coordinated attack on environmental pollution in cooperation with state and local governments.

The Council on Environmental Quality was established within the Executive Office of the President by the National Environmental Policy Act of 1969 to formulate and recommend national policies to promote the improvement of the quality of the environment.

The council:

- Develops and recommends to the president national policies that further environmental quality.
- Performs a continuing analysis of changes or trends in the national environment.
- Reviews and reappraises programs of the federal government to determine their contributions to sound environmental policy.
- Conducts studies, research, and analysis relating to ecological systems and environmental quality.

- Assists the president in the preparation of the annual environmental quality report to the Congress.
- Oversees implementation of the National Environmental Policy Act.

(i) Air and Radiation

The air activities of the EPA include:

- Development of national programs, technical policies, and regulations for air pollution control.
- Enforcement of standards.
- Development of national standards for air quality, emission standards for new stationary and mobile sources, and emission standards for hazardous pollutants.
- Technical direction, support, and evaluation of regional air activities.
- Provision of training in the field of air pollution control.

Related activities include technical assistance to states and agencies having radiation protection programs, including radon mitigation programs, and a national surveillance and inspection program for measuring radiation levels in the environment.

(ii) Water

The EPA's water quality activities represent a coordinated effort to restore the nation's waters. The functions of this program include:

- Development of national programs, technical policies, and regulations for water pollution control and water supply, ground water protection, marine and estuarine protection.
- Enforcement of standards.
- Water quality standards and effluent guidelines development.
- Technical direction, support, and evaluation of regional water activities.
- Development of programs for technical assistance and technology transfer.
- Provision of training in the field of water quality.

(iii) Solid Waste and Emergency Response

The Office of Solid Waste and Emergency Response provides policy, guidance, and direction for the agency's hazardous waste and emergency response programs. The functions of these programs include:

- Development of policies, standards, and regulations for hazardous waste treatment, storage, and disposal.
- National management of the Superfund toxic waste cleanup program.
- Development of guidelines for the emergency preparedness and "community right-to-know" programs.
- Development of guidelines and standards for underground storage tanks.
- Enforcement of applicable laws and regulations.

- Analysis of technologies and methods for the recovery of useful energy from solid waste.
- Provision of technical assistance in the development, management, and operation of waste management activities.

(iv) Pesticides and Toxic Substances

The Office of Pesticides and Toxic Substances is responsible for:

- Developing national strategies for the control of toxic substances.
- Directing the pesticides and toxic substances enforcement activities.
- Developing criteria for assessing chemical substances, standards for test protocols for chemicals, rules, and procedures for industry reporting and regulations for the control of substances deemed to be hazardous to man or the environment.
- Evaluating and assessing the impact of existing chemicals, new chemicals, and chemicals with new uses to determine the hazard and, if needed, develop appropriate restrictions.

Additional activities include control and regulation of pesticides and reduction in their use to ensure human safety and protection of environmental quality. This includes:

- Establishing tolerance levels for pesticides that occur in or on food.
- Monitoring pesticide residue levels in food, humans, and nontarget fish and wildlife and their environments.
- Investiging pesticide accidents.

The Office of Pesticides and Toxic Substances also coordinates activities under its statutory responsibilities with other agencies for the assessment and control of toxic substances and pesticides.

(c) Specific Trade Legislation and Regulations

(i) Tied Aid Practices

"Tied aid" refers to foreign assistance that is linked to the purchase of exports from the country extending the assistance. Tied aid can consist of foreign aid grants alone, grants mixed with commercial financing or official export credits (mixed credits), or concessional (low-interest-rate) loans.

MIXED CREDITS

Mixed credits are a combination of subsidized loans and commercial loans that, in effect, subsidize the purchase of a country's exports.

Competitors' tied aid practices are of concern to the United States because U.S. exporters can be put at a competitive disadvantage in bidding on overseas projects when competitor countries make tied aid available. The effect is the same for any exporting country.

The Organization for Economic Cooperation and Development (OECD) is a forum for monitoring economic trends and coordinating economic policy among its 24 member countries, which include the economically developed free market democracies of North America, Western Europe,

and the Pacific. Negotiators representing countries in the OECD have agreed to curb the use of tied aid for commercial purposes and are taking steps to reduce the use of mixed credits.

(ii) U.S. Export-Import Bank

Exports play a vital role in any economy by creating jobs and generating economic growth. Most industrialized nations have programs to help companies export—that is, sell their products abroad. These programs, collectively referred to as export promotion, include offering business counseling and training and giving representational assistance as well as providing market research information, trade fair opportunities, and export financing assistance. These programs can play an important role in increasing the exports of a country's goods and services in sectors of the economy in which it is competitive.

BUDGET DEFICIT

Budget deficit reduction and liberalized trade are important to the long-term health of any economy.

The U.S. Export-Import Bank (Eximbank) is one of 10 federal government agencies that offer programs to assist exporters. The Eximbank offers a wide range of export financing assistance, including direct loans, loan guarantees, and export insurance covering credit and political risks. Credit risk is the probability that a loan will not be repaid by a foreign country. Political risk is the probability that a foreign country's political system is unstable. Although the Eximbank was created to facilitate the financing of both U.S. exports and imports, it has been used almost exclusively to finance U.S. exports.

The Eximbank is required to counter competitors' use of tied aid and mixed credits. In 1986, the U.S. Congress authorized the Eximbank to create a war chest fund as a means of overmatching or outbidding other countries that have repeatedly used tied aid and mixed credits to increase their exports. However, war chest funds have not been used extensively.

The export promotion programs are effective when:

- U.S. firms lack export awareness because markets have failed to give the right information to producers who otherwise would export.
- U.S. businesses are aware of export opportunities but need additional technical assistance to consummate export sales.
- U.S. firms need representational assistance from the U.S. government in opening doors overseas.
- U.S. businesses need competitive financing, loan guarantees, or insurance to close an export deal.

KEY CONCEPTS TO REMEMBER: Imports and Exports

- Import quotas differ from tariffs. Quotas discriminate on the basis of quantity whereas tariffs directly increase prices.
- GNP will fall following an increase in imports.
- A deficit in the balance of payments occurs when imports exceed exports.

(iii) Methods, Restrictions, and Barriers of International Trade

A country will have a trade deficit when it consumes more than it produces and imports the difference from other countries. A country will become a debtor nation when there is a huge trade deficit and when it borrows to finance the domestic budget deficit.

A country should strike a balance between the national savings rate and the budget deficit, specifically by reducing the deficit without endangering long-term economic growth. An imbalance is created when the savings rate is declining and the budget deficit is increasing. The national savings rate should be sufficient to meet the needs of both private sector investments and government borrowing. A country should focus on long-term investment as a way to enhance its competitiveness in the global marketplace.

A government's economic policies require a difficult balancing of domestic goals with international economic objectives and constraints. For example, at the macroeconomic level, a government may adopt policies that:

- Support private sector investment by keeping the cost of capital at reasonable levels.
- Support rising productivity in the private sector by improving infrastructure and a better-educated and trained labor force.
- Encourage private sector firms to improve their own goals, policies, and management control and information systems as their critical contribution to enhancing their country's competitiveness.

(A) Methods of Restricting Trade Tariffs, import quotas, and domestic content laws are methods used to restrict foreign trade (see Exhibit 8.7).

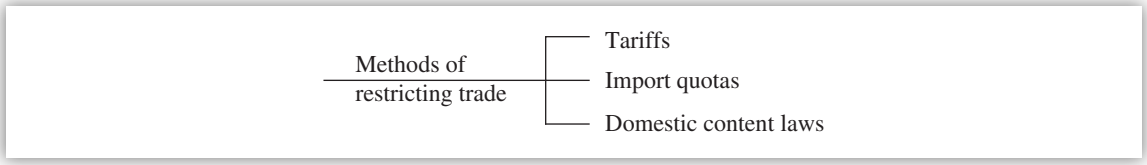


EXHIBIT 8.7 Methods of Restricting Trade

Tariffs A tariff is a tax imposed on imported goods, usually as a percentage of the product's value. Import duties, or tariffs, have been a source of government revenue far longer than income and value-added taxation (VAT). Goods entering a country are taxed at an *ad valorem* (percentage of value) basis. Many foreign countries prefer to use tariffs since it is relatively easy to check and control as goods come through designated ports.

Another popularity of tariffs is its incentive feature to relocate manufacturing production facilities and be competitive. If an American firm exporting to Brazil finds that its products are priced much higher in Brazil because of tariffs, it may build a manufacturing plant in Brazil to produce for the Brazilian market. This strategy has dual benefits: It not only avoids the tariffs to be paid but also makes the American firm's products more competitive in Brazil.

The imposition of a tariff against an imported good raises its cost relative to what it would have been in the tariff's absence. Importers, therefore, need to charge a higher price to their customers. As a consequence, tariffs tend to worsen an imported product's competitive position compared with similar items produced domestically.

Because of high prices of imported goods due to tariffs, more sales will go to local manufacturers. Thus, tariffs offer a degree of market protection to local sellers whose life has been made competitively difficult by imports in their markets. For this reason, when imports become an important factor in a market, domestic manufacturers frequently ask the government for tariff protection. The usual argument is that imports are injuring the local industry and causing unemployment.

Import Quotas A quota is simply a quantitative restriction applied to imports. Under GATT, import quotas are supposed to be banned, but there are so many exceptions that the ban is not that useful. In fact, as tariffs have been reduced as an instrument of protection, the tendency has been to replace them with quotas.

Domestic Content Laws Another way many countries have attempted to ensure the participation of domestic producers has been through domestic content laws. These laws stipulate that when a product is sold in the marketplace, it must incorporate a specified percentage of locally made components. These laws must meet local content requirements.

KEY CONCEPTS TO REMEMBER: Trade

- Consumption taxes on imported goods are an example of a tariff.
- Import tariffs have the same economic effect as a consumption tax plus a production subsidy. A direct effect of imposing a protective tariff on an imported product is lower domestic consumption of the item.
- The merchandise trade balance (or balance of trade) does not reflect capital outflows.
- The point price elasticity of demand for imports will become larger following an increase in import prices.
- A nation experiencing chronic trade deficits might consider trade quotas. Unemployment and productivity rates will decline as a result of trade quotas.
- Increased total world output provides the best justification for reducing trade barriers between nations.
- An embargo creates the most restrictive barrier to exporting to a country and often results from political actions. An embargo is a total ban on some kind of imports, which is an extreme form of import quota.

(B) Methods of International Trade Export promotion programs, trade agreements, and technology policies set the stage for international trade to occur.

Export Promotion Programs As each country's economic advancement is dependent on its success in trading with other countries, the way that country promotes its exports will be of great importance. Therefore, it is important to ensure that the funds allocated are being channeled into areas with the greatest potential returns. A budget for export promotion programs would be a good start. For a government to promote these programs requires good internal controls, program evaluation criteria, proper program accountability, and enhanced planning and decision making. *Export promotion programs, export loans, credit guarantees, and insurance are some examples of promoting international trade.*

Trade Agreements Two popular trade agreements are the WTO, formally known as GATT and NAFTA. The aim of U.S. trade negotiations is to remove foreign barriers to imports and unfair governmental incentives to exports, thus encouraging the free flow of international trade. The principal multinational trade regime has been the WTO, which requires the negotiations of concerned countries in liberalizing the trade and removing tariffs and other barriers—which is not an easy thing to accomplish. More is said about WTO later.

TRADE AGREEMENTS

A vigorous and effective system for monitoring and enforcing agreements is essential to avoid violations, delaying tactics, and drawn-out dispute settlements.

The United States, Mexico, and Canada concluded negotiations and signed the NAFTA, which became effective in 1994. The most significant aspect of NAFTA is that it binds Mexico's market-oriented economic reforms to international obligations, thereby making these reforms more permanent. Although NAFTA will likely have only a modest net effect on the U.S. economy, much controversy remains as to the scope and extent of social and economic adjustments that will be caused by its implementation, such as effects on employment, immigration, and the environment. More is said about NAFTA later.

Technology Policies Technology policies, the financial market structures, and the business/government relationships of other nations will have greater significance in the more closely integrated global marketplace.

The U.S. International Trade Commission furnishes studies, reports, and recommendations involving international trade and tariffs to the president, the Congress, and other government agencies. In this capacity, the commission conducts a variety of investigations, public hearings, and research projects pertaining to the international policies of the United States.

EXERCISE ON TRADE BARRIERS

The United States imposed many barriers to international trade during the 1920s and 1930s. The United States has become much less protectionist and has eliminated or lessened numerous former barriers to trade. In the last several years, as a result of increased foreign competition in some historically strong U.S. industries, some observers have become concerned that the United States will extend protection to other industries.

Question: Describe the basic types of trade barriers.

Answer: *The three basic types of trade barriers include tariffs, quotas, and other nontariff barriers.* A **tariff** is an import tax that may be used as a source of revenue for the government. A **quota** is a physical or dollar value limitation on the volume of imports of a particular commodity. A quota generates no revenue for the government, but it generates monopoly profits for the protected industry. A quota also increases the burden of adjustment of prices relative to tariffs. **Other nontariff barriers** include an array of government practices and regulations that interfere with the free flow of goods between countries. Some of the most common nontariff barriers include: export subsidies and taxes, differences in product standards, domestic subsidies and aids, and dumping regulations and customs valuations procedures.

Question: For each type, describe the impact on the protectionist country (importer) imposing the barrier.

Answer: All of the trade barriers are designed to decrease the quantity of imported goods supplied either by increasing prices or directly restricting quantities causing subsequent price increases. A tariff works by raising prices and hence cutting the demand for imports while quotas restrict the supply of imports forcing prices up. The increase in price associated with a tariff does not directly benefit the seller; it becomes a source of revenue for the importing country. The increase in price associated with a quota does not become a source of revenue for the importing country, but the benefits become the property rights of some participant in the market yielding monopoly profits. The degree of protection that is achieved is determined by the demand elasticity of the product and whether the exporting country imposes retaliatory trade barriers.

Question: Describe the impact on producer nations (exporter) facing the barrier.

Answer: Tariffs, quotas, and other nontariff barriers cause the volume of trade to decline. Since products can no longer be exported as profitably, prices will decline in the exporting country. Production will decrease in the exporting country resulting in a loss of income.

Question: Describe the impact on international trade in the year-end balance of payments between the protectionist and the producer.

Answer: In the importing country, the balance of payments improves. In the exporting country, the balance of payments worsens.

Source: Institute of Internal Auditors, *CIA Examination*, Part IV, Question No. 42 (Altamonte Springs, FL: May 1986).

(iv) Theory of Comparative Advantage

Increased total world output is a good argument for free trade between countries. Incentives exist for trade to develop along the lines of comparative advantage. Countries achieve comparative advantage in certain goods due to international differences in demand or supply.

The law of comparative advantage explains how mutually beneficial trade can occur when one country is less efficient than another county in the production of all commodities. The less efficient country should specialize in and export the commodity in which its absolute disadvantage is smallest and should import the other commodity.

Countries should specialize when they have their greatest absolute advantage or in their least absolute disadvantage. This rule is known as the law of comparative advantage. An absolute advantage is the ability to produce a good using less input than is possible anywhere else in the world.

Production of the good with the lower price expands, and the country with a lower relative price of a product has comparative advantage in that product. Therefore, production and trade follow the line of comparative advantage. For trade to occur along the lines of comparative advantage, the relative wage ratio must lie between the extremes of the differences in relative productive advantages.

The **HO theorem** states that a country will have a comparative advantage in and therefore will export that good whose production is relatively intensive in the factor with which that country is relatively well endowed. For example, a country that is relatively capital-abundant compared with another country will have a comparative advantage in the good that requires more capital per worker to produce.

In a competitive environment, trade flows are determined by profit-seeking firms. If a product is relatively cheap in one country, it will tend to be exported to those places where it is relatively expensive. This practice supports the assumption that trade will flow in the direction of comparative advantage. *Each country exports its comparative-advantage good and imports its comparative-disadvantage good.*

EXAMPLES OF COMPARATIVE ADVANTAGE THEORY

Example 1

Country A		Country B	
Good X	**Good Y**	**Good X**	**Good Y**
100	0	60	0
60	20	30	10
20	40	0	20
0	50		

This table represents production possibilities for Country A and Country B for two goods, X and Y. Based on the principle of comparative advantage, Country B should produce Good X.

Example 2

	Country A	Country B
Cotton	3	12 labor hours per unit of output
Automobile	6	8

Note that Country A is four times (i.e., 12 to 3) more efficient in the production of cotton relative to Country B. However, Country A is only 4/3 (i.e., 8/6) more efficient in the production of automobiles relative to Country B. Because Country A's greatest absolute advantage is in the production of cotton, it is said to have a comparative advantage in cotton. Because Country B's least absolute disadvantage is in the production of automobiles, it is said to have a comparative advantage in automobiles.

Example 3

Assume a simple economy consisting of only two nations, Nation A and Nation B. The countries produce and consume only two products: rice and cars. The comparative costs of production in each country are

	Nation A	Nation B
Rice (per ton)	10,000	20,000
Cars	15,000	16,000

Given this cost structure and a fixed supply of inputs, what can be said with respect to comparative advantage and international trade?

a. Nation B has a comparative advantage with respect to the production of cars and will export cars to Nation A.
b. Nation B has a comparative advantage with respect to rice and will export rice to Nation A.
c. Nation A has a comparative advantage with respect to cars and will export cars to Nation B.
d. There will be no overall advantage to international trade.

Choice (a) is the correct answer. Nation B has a comparative advantage in cars because the within-country price comparison between cars and rice is lower for Nation B (16,000/20,000 = 0.8) than for Nation A (15,000/10,000 = 1.5). Nation A has an absolute advantage, but Nation B has the comparative advantage. Choice (b) is incorrect. Nation A has the comparative advantage for rice because its cost relationship (10,000/15,000 = 0.667) is lower than in Nation B (20,000/16,000 = 1.25). Choice (c) is incorrect. Nation B has the comparative advantage for cars. Choice (d) is incorrect. Total output will be maximized when each nation specializes in the products in which it has the greatest comparative advantage.

(v) International Laws

Laws regarding WTO, NAFTA, the EU, and other regional groups are discussed in this section.

(A) World Trade Organization The Final Act resulting from the Uruguay Round of negotiations of the GATT was signed in April 1994. The Final Act created a new WTO as a successor to GATT. WTO would bring all member countries under more of the multilateral trade disciplines.

Implementation of the Uruguay Round agreement is meant to:

- Further open markets by reducing tariffs worldwide by one-third.
- Improve GATT procedures over unfair trade practices.
- Broaden GATT coverage by including areas of trade in services, IP rights, and trade-related investment that previously were not covered.
- Provide increased coverage to the areas of agriculture, textiles and clothing, government procurements, and trade and the environment.

WTO STRUCTURE

The agreement establishing the World Trade Organization would, for the first time, create a formal organization encompassing all GATT disciplines. WTO membership would be open only to countries that agree to adhere to all of the Uruguay Round agreements and submit schedules of market access commitments for industrial goods, agricultural goods, and services. As such, this agreement would resolve the free rider problem and permit members to cross-retaliate by suspending concessions under any of these agreements when authorized to impose sanctions. Adherence to the four plurilateral agreements would not be mandatory.

Free Rider Problem

Due to the WTO's MFN requirements, member countries that adhere to a given code and provide concessions in accordance with its obligations are required to accord the same benefits to all WTO members, including those countries that did not adhere to the code and thus do not reciprocate.

Inability to Cross-Retaliate

When a WTO member country is authorized to impose sanctions against another member for violating its obligations under a given code, it may only suspend concessions provided under that code. This restriction limits the plaintiff country's options and may make it difficult for that country to devise an effective sanction.

The agreement also makes provision for improved cooperation with other multilateral organizations with responsibilities and concerns similar to WTO, such as the World Bank and International Monetary Fund (IMF) as well as the OECD. It also would establish within WTO a Trade Policy Review Board comprised of the members. This review body would examine, on a regular basis, national trade policies and other economic policies affecting the international trading environment.

Agreement for Market Access The market access for goods agreement is a key part of the Uruguay Round's overall goal of liberalizing international trade by further opening markets among WTO countries. It is essentially a tariff schedule that reflects the concessions agreed on by WTO signatories. The main contribution of the market access agreements would be to significantly lower, or eliminate, tariff and nontariff barriers and to expand the extent of tariff bindings on industrial products among WTO signatories. The global economic impact of this agreement is substantial.

Provisions for Subsidies and Countervailing Duties Subsidies essentially lower a producer's costs or increase its revenues. Consequently, producers may sell their products at lower prices than their competitors from other countries. Subsidies to firms that produce or sell internationally traded products can distort international trade flows.

The United States has historically provided fewer industrial subsidies than most countries, and it has sought to eliminate trade-distorting subsidies provided by foreign governments.

Countervailing duty laws can address some of the adverse effects that subsidies can cause. Countervailing duties are special customs duties imposed to offset subsidies provided on the manufacture, protection, or export of a particular good.

The agreement would create for the first time three categories of subsidies and remedies: (1) prohibited subsidies (the red light category); (2) actionable subsidies (the yellow light category); and (3) nonactionable subsidies (the green light category) (see Exhibit 8.8).

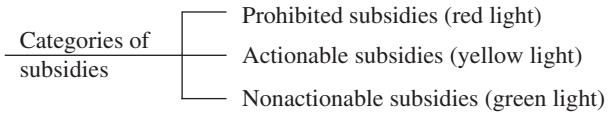


EXHIBIT 8.8 Categories of Subsidies

Prohibited subsidies include subsidies to encourage exports, including de facto export subsidies, and subsidies contingent on the use of local content.

Actionable subsidies are domestic subsidies against which remedies can be sought if they are shown to distort trade. Trade distortion occurs if: subsidized imports cause injury to a domestic industry (e.g., depress prices or threaten to do so); subsidies nullify or impair benefits owed to another country under WTO (e.g., the benefits of bound tariff concessions); or subsidized products displace or impede imports from another country or another country's exports to a third-country market.

There is also a special category of actionable subsidies that have a high likelihood of being trade distorting. These subsidies are presumed to cause "serious prejudice" to the trade interests of other countries when *either* of the following conditions are met:

- The total ad valorem subsidization of a product exceeds 5% of the value of the firm's or industry's output of a product (calculate on the basis of cost to the subsidizing government).
- Subsidies are provided to forgive debts or subsidies cover a firm's or an industry's operating losses.

In cases where serious prejudice is presumed, the burden is on the subsidizing government to demonstrate that serious prejudice did not result from the subsidy in question.

Nonactionable subsidies include those that are not "specific" (i.e., not limited to an enterprise or industry or group of enterprises or industries). Subsidies also are nonactionable if they involve certain government assistance: for research and precompetitive development activity, for disadvantaged regions, or to adapt existing plants and equipment to new environmental requirements.

Provision for Antidumping Dumping is generally considered to be the sale of an exported product at a price lower than that charged for the same or a like product in the home market of the exporter. This practice is thought of as a form of price discrimination that can potentially harm the importing nation's competing industries.

Dumping may occur as a result of exporter business strategies that include:

- Trying to increase an overseas market share.
- Temporarily distributing products in overseas markets to offset slack demand in the home market.
- Lowering unit costs by exploiting large-scale production.
- Attempting to maintain stable prices during periods of exchange rate fluctuations.

International trade rules, as defined by WTO, take political as well as economic concerns into account and view dumping and its potential harm broadly. Article VI of the WTO agreement notes that the contracting parties recognize that dumping "is to be condemned if it causes or threatens material injury to an established industry in the territory of a contracting party or materially retards the establishment of a domestic industry." The rules allow for the imposition of antidumping duties, or fees, to neutralize the injurious effect of these pricing practices.

Some trade economists view dumping as harmful only when it involves the use of "predatory" practices that intentionally try to eliminate competition and gain monopoly power in a market. They believe that predatory dumping rarely occurs and that antidumping enforcement is a protectionist tool whose cost to consumers and import-using industries exceeds the benefits to the industries receiving protection. Moreover, they believe that increased use of antidumping protection effectively reduces the anticipated gains that trade liberalization through tariff reduction will realize for the national economy.

Provision for Safeguards A safeguard is a temporary import control or other trade restriction a country imposes to prevent injury to domestic industry caused by increased imports. Article

19 of the current GATT agreement, known as the safeguard clause, allows contracting parties to obtain emergency relief from import surges. It is designed to help the domestic industries adjust to an influx of fairly traded imports.

The new Safeguard Agreement would require that safeguard measures be limited to an eight-year period for developed countries and ten years for developing countries. It provides for suspending the automatic right to retaliate to a safeguard measure for the first three years. However, it would maintain the requirement that safeguards be applied on an MFN basis rather than being applied selectively (applied to just the country or countries causing injury to the domestic industry).

Agreement on Trade-Related Aspects of IP Rights The World Intellectual Property Organizations (WIPO), a United Nations specialized agency, is a world body whose mission is to (1) promote the protection of IP rights throughout the world through cooperation among countries and, where appropriate, in collaboration with international organizations; and (2) ensure administrative cooperation among the IP unions. WIPO administers a number of international agreements on IP protection, including, in particular, the Berne Convention for the Protection of Literary and Artistic Works, which provides for copyright protection, and the Paris Convention for the Protection of Industrial Property, which provides protection for patents, trademarks, and industrial designs and the repression of unfair competition.

According to U.S. officials, these conventions do not contain specific commitments in important areas. For example, the Paris Convention does not contain a required minimum length of time for patent protection or specify the subject matter to be covered by patents, and the Berne Convention does not provide copyright protection for newer creations, such as sound recordings. Further, they do not provide for meaningful enforcement measures, an area long considered crucial by U.S. interests; the Industry Functional Advisory Committee on IP rights has pointed out that standards of protection are useless unless they are enforced.

Agreement on Trade in Services Service industries dominate the U.S. economy and are important contributors to U.S. exports. The U.S. service industry is also the world's largest exporter of services. International trade in services takes place through various channels, including:

- Cross-border transactions, such as transmission of voice, video, data, or other information and the transportation of goods and passengers from one country to another.
- Travel of individual consumers to another country (e.g., services provided to nonresident tourists, students, and medical patients).
- Sales of services (e.g., accounting, advertising, and insurance) through foreign branches or other affiliates established in the consuming country.
- Travel of individual producers to another country (e.g., services provided to foreign clients by business consultants, engineers, lawyers, etc.).

The Uruguay Round meetings created General Agreement on Trade in Services (GATS), which is the first multilateral, legally enforceable agreement covering trade and investment in the services sector.

Agreement on Trade-Related Investment Measures There is consensus among many, primarily developed, countries that foreign direct investment can have a favorable effect on a host country's

economy. The foreign direct investment can create jobs, increase tax revenues, and introduce new technologies. It also increases the host country wages and productivity and seems to have a net positive effect on the competitiveness of the host economy.

According to the U.S. Department of Commerce review of foreign direct investment, firms choose to expand their activities overseas for a variety of reasons. These reasons include a desire to:

- Maintain profitability while reducing prices when faced with lower competitors' prices.
- Maintain an increased worldwide market share.
- Gain access to or retain access in an overseas market, especially in periods when trade restrictions are threatened.
- Exploit, and maintain control over, an advantage specific to a company, such as management, marketing, and/or technology, or a comparative advantage in producing in the foreign market.
- Improve the company's ability to meet the overseas market's needs by providing a special product design and/or service.

The WTO created trade-related investment measures (TRIMs), which have economic effects that are comparable to those of traditional instruments of commercial policy, such as quotas, tariffs, and subsidies. TRIMs exist in many forms. TRIMs include local content requirements (obliging an investor to purchase or use a specified amount of inputs from local suppliers). Local content requirements are the most common form of TRIM and are used in an attempt to ensure that the investment increases local employment and develops physical and human capital. TRIMs also include trade-balancing requirements. TRIMs are placed on foreign direct investment by governments in an effort to: influence investment decisions such as sourcing, production, and market locations; increase the likelihood that the host nation will capture the benefits expected from the investment; and redistribute the investment benefits from the investor to the host country.

TRIMs can be implemented in different ways. They can be mandatory, that is, enforceable under domestic law or administrative rulings. An example of this type of mandatory TRIM would be a law that states that investors must include a certain percentage of local content in their production. In addition, TRIMs can be actions that are necessary for an investor to undertake in order to obtain some type of advantage (investment incentive)—a quid pro quo approach. For example, a host government might approach an investor with a proposal that allows the investor to receive a tax exemption in return for including a certain percentage of local content in the company's production.

Agriculture Provisions of the Uruguay Round The Uruguay Round represented the first time that WTO contracting parties undertook to substantially reform agricultural trade. The Punta del Este ministerial declaration recognized an urgent need to stabilize the world agriculture market and liberalize trade by reducing import barriers, discipling the use of direct and indirect subsidies that affect trade, and minimizing the adverse effect of sanitary and phytosanitary regulations and barriers. The declaration recognized that other negotiating areas were likely to improve agricultural trade as well, such as efforts to strengthen the dispute resolution process. The sanitary and phytosanitary regulations and barriers are measures taken to protect human, animal, or plant life or health.

(B) North American Free Trade Agreement NAFTA, which went into effect on January 1, 1994, was intended to facilitate trade and investment throughout North America (United States, Canada, and Mexico). It incorporates features such as the elimination of tariff and nontariff barriers. NAFTA also supports the objective of locking in Mexico's self-initiated, market-oriented reforms. By removing barriers to the efficient allocation of economic resources, NAFTA was projected to generate overall, long-term economic gains for member countries—modest for the United States and Canada and greater for Mexico. For the United States, this is due to the relatively small size of Mexico's economy and because many Mexican exports to the United States were already subject to low or no duties. Under NAFTA, intra-industry trade and coproduction of goods across the borders were expected to increase, enhancing specialization and raising productivity.

NAFTA also included procedures first to avoid, and then to resolve, disputes between parties to the agreement. Separately, the three NAFTA countries negotiated and entered into two supplemental agreements designed to facilitate cooperation on environment and labor matters among the three countries. NAFTA will create the largest free trade zone in the world, with 360 million people and an annual gross national product totaling over $6 trillion dollars.

Major Provisions of NAFTA Major provisions are listed next.

- Rules of origin
- Import/export quotas and licenses
- Technical standards and certification
- Escape clauses
- Telecommunications networks
- Cross-border trade in services
- Antidumping and subsidy laws
- Cross-subsidization
- Investments
- Performance requirements
- Right to convert and transfer local currencies
- Disputes
- IP rights
- Due process
- Temporary entry visas
- Side agreements

Rules of Origin NAFTA trade is subject to rules of origin that determine whether goods qualify for its tariff preferences. These include goods wholly originating in the free trade area. A general waiver of the NAFTA rules of origin requirements is granted if their nonregional value consists of no more than 7% of the price or total cost of the goods. Regional value may be calculated in most cases either by a transaction value or a net cost method. The former avoids costly accounting systems. The latter is based on the total cost of the goods less royalties, sales promotion,

packing and shipping, and allowable interest. Either method will require manufacturers to trace the source of non-NAFTA components and maintain source records.

Import/Export Quotas and Licenses Import and export quotas, licenses, and other restrictions will gradually be eliminated under NAFTA subject to limited rights to restrain trade—for example, to protect human, animal, or plant health or to protect the environment.

Technical Standards and Certification Technical standards and certification procedures for products are classic examples of nontariff trade barriers. Mutual recognition of professional license is encouraged (notably for legal consultants and engineers) but not made automatic. All three countries have agreed not to lower existing environmental or health and safety standards in order to attract investments and will attempt to "upwardly harmonize" them. Environmental impact statements for foreign investments are required.

Escape Clauses Escape clause rules and procedures are applicable to United States–Mexico trade under NAFTA. These permit temporary trade relief against import surges subject to a right of compensation in the exporting nation.

Telecommunications and Networks Public telecommunications networks and services must be opened on reasonable and nondiscriminatory terms for firms and individuals who need the networks to conduct business.

Cross-Border Trade in Services Cross-border trade in services is subject to national treatment, including no less favorable treatment than that most favorably given at federal, state, or local government levels. Existing cross-border restraints on the provision of financial services are frozen, and no new restraints may be imposed. Providers of financial services in each NAFTA nation will receive both national and MFN treatment. This includes equality of competitive opportunity, which is defined as avoidance of measures that pose a disadvantage to foreign providers relative to domestic providers.

Various procedural transparency rules are established to facilitate the entry and equal opportunity of NAFTA providers of financial services. The host nation may legislate reasonable prudential requirements for such companies and, under limited circumstances, protect its balance of payments in ways that restrain financial providers.

Antidumping and Subsidy Laws Antidumping and subsidy laws and countervailing duties are applicable. A special committee may be invoked if the opportunity for independent judicial review on a dumping or subsidy determination has been denied.

Cross-Subsidization Cross-subsidization between public transport services is not prohibited, nor are monopoly providers of public networks or services.

Investments Investment in the industrial and services sectors of the NAFTA nations is promoted through rules against nondiscriminatory and minimum standards of treatment that benefit even non-NAFTA investors with substantial business operations in a NAFTA nation.

Performance Requirements Performance requirements—for example, specific export levels, minimum domestic content, domestic sources preferences, trade balancing, technology transfer, and product mandates—are disallowed in all areas except government procurement, export promotion, and foreign aid.

Senior management positions may not be reserved by nationality, but NAFTA states may require that a majority of the board of directors or committees thereof be of a designated nationality of residence, provided this does not impair the foreign investor's ability to exercise control.

Right to Convert and Transfer Local Currencies A general right to convert and transfer local currency at prevailing market rates for earnings, sale proceeds, loan repayments, and other investment transactions has been established. Direct and indirect expropriations of investments by NAFTA investors are precluded except for public purposes and if done on a nondiscriminatory basis following due process of law. A right of compensation without delay at fair market value plus interest is created.

Disputes In the event of a dispute, a NAFTA investor may elect monetary (but not punitive) damages through binding arbitration in the home state of the investor or pursue judicial remedies in courts of the host state.

Investment, dumping, and subsidy, financial services, environmental-investment, and standards disputes are subject to special dispute resolution procedures. A right of consultation exists when one country's rights are affected.

IP rights NAFTA mandates adequate and effective IP rights in all countries, including national treatment and effective internal and external environment rights.

For copyright, NAFTA obligates protection for computer programs, database, computer programs, and sound recording rentals and a 50-year term of protection for sound recordings. For patents, NAFTA mandates a minimum 20 years of coverage of nearly all products and processes, including pharmaceuticals and agricultural chemicals. Compulsory licensing is limited, notably regarding pharmaceuticals in Canada. Service marks are treated equally with trademarks. Satellite signal poaching is illegal and trade secrets are generally protected. NAFTA details member states' duties to provide damages, injunctive, antipiracy and general due process remedies in the IP field.

Due Process An agreement exists that deals with general duty of legal transparency, fairness, and due process regarding all laws affecting traders and investors with independent administrative or judicial review of governmental action. Generalized exceptions to the agreement cover actions to protect national security and national interests, such as public morals, health, national treasures, and natural resources, or to enforce laws against deceptive or anticompetitive practices, short of arbitrary discriminations or disguised restraints on trade.

Balance of payments trade restraints are governed by the rules of the International Monetary Fund (IMF). Taxation issues are subject to bilateral double taxation treaties, including a new one between Mexico and the United States.

Temporary Entry Visas Entry rights cover businesspersons, traders, investors, intracompany transferees, and 63 designated professionals. White-collar businesspersons only need proof of citizenship and documentation of business purpose to work in another NAFTA country for up to five years. However, an annual limit of 5,500 additional Mexican professionals may temporarily enter the United States during the first 10 years of NAFTA. Apart from these provisions, there is no common market for the free movement of workers.

Side Agreements Side agreements on labor and the environment commit each country to create environmental and labor commissions that monitor compliance with the adequacy and the

enforcement of domestic law. These commissions are empowered to receive complaints. Negotiations to resolve complaints would ensue. Absent a solution, an arbitral panel of experts from the three nations would be convened to evaluate the complaint.

Impacts and Implementation of NAFTA Assessment of NAFTA's effects is a complex undertaking since the provisions last 10 to 15 years. While NAFTA is not yet fully implemented, U.S. trade with NAFTA members has accelerated and is in accordance with pre-NAFTA expectations.

At the sector level, there are diverse impacts from NAFTA. Within sectors, these impacts may include increases or decreases in trade flows, hourly earnings, and employment. Economic efficiency may improve from this reallocation of resources, but it creates costs for certain sectors of the economy and labor force, including job dislocation.

In general, NAFTA or broader trade policies cannot be expected to substantially alter overall U.S. employment levels, which are determined largely by demographic conditions and macroeconomic factors such as monetary policy.

While there is wide conceptual agreement on how trade liberalization contributes to improvement in the standard of living through increased productivity and lower prices, estimating the extent to which NAFTA specifically furthers these goals presents a major empirical challenge. For example, there are no estimates of NAFTA's direct impact on productivity. However, growth in shared production activity and two-way trade suggests that increases in sector specialization, a mechanism through which productivity may be improved, have occurred.

NAFTA's system for avoiding and settling disputes among the member countries is a critical element of the agreement. The agreement includes mechanisms such as the establishment of committees and working groups and an early consultation process to help the parties avoid disputes. These mechanisms have helped the governments resolve important trade issues and have kept the number of formal dispute settlement cases relatively low.

Trade laws agreed to under NAFTA have helped members improve the transparency (openness) of their antidumping and countervailing duty administrative processes, thus reducing the potential for arbitrariness in their application.

It is too early to determine what definitive effect the supplemental agreements will have on the North American environment and labor. However, some government and private sector officials have acknowledged that the two commissions created to implement the agreements have been for several positive achievements to date.

(C) European Union The EU, often called the Common Market, is a supranational legal regime with its own legislative, administrative, treaty-making, and judicial procedures. To create this regime, 15 or more European nations have surrendered substantial sovereignty to the EU. EU law has replaced national law in many areas, and the EU legal system operates as an umbrella over the legal systems of the member states. EU law is vast and intricate. The EU has an aggregate population exceeding 375 million and a GNP exceeding $7,000 billion. The EU is the largest market for exports from the United States.

The tasks of the EU include creation of an economic and monetary union with emphasis on price stability with the goal of establishing a Europe "without internal frontiers."

The Council, the Commission, the Parliament, the Court of Justice The **Council** consists of representatives of the ruling governments of the member states. The European Community Treaty requires the Council to act by a qualified majority on some matters and with unanimity on others.

The **Commission** is independent of the member states. Its 20 commissioners are selected by council appointment. They do not represent member states or take orders from member state governments. The Commission is charged with the duty by acting only in the best interests of the EU and serves as the guardian of the treaties. The Commission largely maintains EU relations with GATT and WTO. It proposes and drafts EU legislation and submits that legislation to the Council for adoption.

The **Parliament** historically played an advisory role. The European Parliament has the power to put questions to the Commission and the Council concerning EU affairs. It also has the power, so far unused, to censure the Commission, in which event all commissioners are required to resign as a body. As a minimum, the Parliament has a right to be consulted and to give an "opinion" as part of the EU legislative process. The opinion is not binding on the Commission or Council.

The role of the **Court of Justice** is to ensure that, in the interpretation and application of the treaty, the law is observed. Fifteen justices (one from each state) make up the European Court of Justice. If a conflict arises between EU law and the domestic law of a member state, the Court of Justice has held that the former prevails. When there is no conflict, both EU law and domestic law can coexist.

Major Provisions of the European Union The major provisions of EU laws include: free movement of goods, of workers, of capital, and of payments; and establishment of a monetary system, a tax system, and trade rules with nonmember states.

Free Movement of Goods The treaty attempts to achieve free movement of goods by establishment of a Customs Union to eliminate, between the member states, customs duties and all other charges having "equivalent effect." It has established a Common Customs Tariff with the outside world. Quantitative restrictions on imports between member states and measures having an equivalent effect are also prohibited. Nontariff trade barriers are frequently the subject of intense negotiation within the EU and remain the most troublesome feature of the Customs Union.

Free Movement of Workers The treaty distinguishes the "free movement of workers" (blue-collar workers and artisans) from the "right of establishment" and "freedom to provide services." Regarding free movement of workers, the treaty prohibits "any discrimination, based on nationality, between workers of the member states as regards employment, remuneration and other conditions of work and employment." Free movement of self-employed persons and of services across member state boundaries is aided by the right of establishment. Restrictions on the freedom to provide services across borders without local establishment are being abolished progressively.

Free Movement of Capital The treaty requires the removal of national restrictions on the free movement of capital belonging to persons of member states "to the extent necessary to insure the proper functions of the Common Market."

Free Movement of Payments The "free" movement of workers and capital should be distinguished from the free movement of payments necessary to EU trade. Current payments are, as a rule, treated more liberally under Union law and indeed are essential to the free movement of goods and services in the Common Market.

Monetary System In movement toward a monetary Union, the member states have created the European Monetary System (EMS) and the European Exchange Rate Mechanism (ERM). The ERM is similar in concept and form to the currency basket, and allows limited fluctuations on national exchange rates from agreed parities.

The states have also established a joint credit facility for giving short- and medium-term financial support to EMS currencies under pressure. The European Currency Unit (ECU) is the basis of definition of the basket parities. ECUs, although not a tangible currency, are used as the basis of settlement between banks within the EMS, for budgetary purposes, to calculate agricultural subsidies, and levy fines and penalties. ECUs are increasingly used as reference values in private transactions.

Tax System With considerable effort, the EU nations have adopted a common tax system called value-added taxation. But different revenue needs and tax policies cause different levels of VAT to apply to like items in the various member states.

The tax frontiers will be eliminated by imposing VAT reporting and collection duties on importers and exporters using the "destination principle" on VAT rates.

Trade Rules The treaty requires member states to coordinate and implement a common commercial policy toward nonmember states. This policy is based on uniform principles regarding tariff and trade agreements, fishing rights, export policy, and other matters of external concern to the EU.

WTO VERSUS NAFTA VERSUS EU

- Due to the WTO's focus on reducing trade barriers, its provisions have more far-reaching long-term effects on the world economy than NAFTA or the EU.
- When there is a conflict between WTO and NAFTA, the latter prevails.
- NAFTA is better streamlined politically, legislatively, and judicially than EU.
- Unlike the EU, there is no NAFTA Council of Ministers, Court of Justice, or Parliament.
- The EU Commission is more powerful than NAFTA's Trade Commission.
- NAFTA goals and techniques are strikingly limited while they are strikingly ambitious for the EU.
- NAFTA's goals are more achievable than those of the EU due to the EU's grand-scale nature.
- NAFTA's treaty is for a limited duration (10 to 15 years) while the EU treaty is of unlimited duration. Any nation in NAFTA may withdraw on six months' notice, and other nations can be admitted to the NAFTA.
- NAFTA's economic integration can advance to greater degrees than that of the EU due to several, different, complex nations involved in the EU.
- The EU has legal foundation while NAFTA has economic foundation.

(D) Other Regional Groups Many nations are contemplating or have already formed regional economic integration to capture the economic gains and international negotiating strength that regionalization can bring. Some regions or groups are listed next.

- Several groups have been formed in Africa including UDEA, CEAO, and ECOWAS. The purpose is to establish a common customs and tariff approach toward the rest of the world and to formulate a common foreign investment trade.
- Regional groups have been established in Latin America and the Caribbean (CARICOM, CACM, LAFTA/LAIA). The Latin American Free Trade Association (LAFTA) had small success in reducing tariffs and developing the region through cooperative industrial sector programs. These programs allocated industrial production among the participating states. In 1994, some 37 nations signed the Association of Caribbean States agreement with long-term economic integration goals.
- Gulf Cooperations Council (GCC) was formed among Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates with these objectives: of establishing freedom of movement, a regional armaments industry, common banking and financial systems, a unified currency policy, a customs union, a common foreign aid program, and a joint, international investment company, the Gulf Investment Corporation. The GCC has implemented trade and investment rules concerning tariffs on regional and imported goods, government contracts, communications, transportation, real estate investment, freedom of movement of professionals, and development of a Uniform Commercial Code. In 1987, the GCC entered into negotiations with the EU that resulted in a major 1990 trade and cooperation agreement.
- The Andean Common Market (ANCOM) was founded by Bolivia, Chile, Colombia, Ecuador, and Peru in 1969 primarily to counter the economic power of Argentina, Brazil, and Mexico and to reduce dependency on foreign capital. Later, Venezuela joined and Chile left the group. The ANCOM Commission has not been an activist on behalf of regional integration like the EU Commission. It mostly reacts to proposals put forth by the Junta, the administrative arm of ANCOM.
- The Association of South East Asian Nations (ASEAN) was formed in 1967 by Indonesia, Malaysia, the Philippines, Singapore, and Thailand. Brunei joined in 1984, and Vietnam joined in 1995. The Bangkok Declaration establishing ASEAN as a cooperative association is a broadly worded document but with little supranational legal machinery to implement its stated goals.
- East Asian Integration, ranging from Japan in the north to Indonesia in the south, has formed Asia-Pacific Economic Cooperation (APEC) consisting of 18 Asian-Pacific nations including the United States. East Asia, unlike Europe, has not developed a formal Common Market with uniform trade, licensing, and investment rules. Late in 1994, the APEC nations targeted free trade and investment for developed countries by the year 2010 and developing countries by the year 2020.

OPTIONS FOR NATIONS

Nations in the world have options to consider prior to joining a group of countries for economic integration. These options are listed next.

- **Free trade areas.** In free trade areas, tariffs, quotas, and other barriers to trade among participating states are reduced or removed while individual national trade barriers vis-à-vis third-party states are retained.
- **Customs unions.** Customs unions not only remove trade barriers among participating states; they also create common trade barriers for all participating states regarding third-party states.
- **Common markets.** Common markets go further than customs unions by providing for the free movement of factors of production (e.g., capital, labor, technology, and enterprise) among participating states.
- **Economic communities.** Economic communities build on common markets by introducing some harmonization of basic national policies related to the economy of the community (e.g., transport, taxation, corporate structure, monetary matters, and regional growth).
- **Economic unions.** Economic unions embrace a more or less complete harmonization of national policies related to the economy of the union (e.g., company laws, commercial treaties, social welfare, currencies, and governmental subsidies). Economic communities and economic unions are different only in regard to the number and importance of harmonized national policies.

8.5 Sample Practice Questions

As mentioned in the Preface of this book, a small batch of sample practice questions is included here to show the flavor of questions and to create a quiz-like environment. The answers and explanations for these questions are shown in a separate section at the end of this book just before the Glossary. If there is a need to practice more questions to obtain a greater confidence, refer to the section "CIA Exam Study Preparation Resources" presented in the front matter of this book.

1. Which type of organization uses a very high degree of local decision making, evaluation, and control?

a. Polycentric

b. Geocentric

c. Ethnocentric

d. Polychronic

2. Which of the following is vital to communication in high-context culture?

a. Being on time

b. Nonverbal and situational cues

c. Being polite

d. Written contacts

3. To enter foreign markets, most firms begin with which of the following strategies?

a. Exporting

b. Licensing

c. Direct foreign investment

d. Joint ventures

4. Which of the following **best** describes a transnational company?

a. Centralized authority and distinct national identity

b. Decentralized authority and distinct national identity

c. Decentralized authority and no distinct national identity

d. Centralized authority and no distinct national identity

5. In addition to the four basic requirements of a contract, which of the following must also occur in order to have a valid contract?

a. The agreement always must be in writing.

b. There must be evidence of undue influence.

c. There must be an absence of an invalidating contract.

d. A legal remedy need not be available for there to be a breach.

6. Some economic indicators lead the economy into a recovery or recession, and some lag it. An example of a lag variable would be:

a. Chronic unemployment.

b. Orders for consumer and producer goods.

c. Housing starts.

d. Consumer expectations.

7. The two main variables that contribute to increases in a nation's real gross domestic product (GDP) are labor productivity and:

a. Definition of the labor force.

b. Inflation rate.

c. Quality of output.

d. Total worker hours.

8. If a country uses trade quotas to overcome chronic trade deficits, the most likely outcome is:

a. Unemployment and productivity rates will rise.

b. Unemployment rates will rise and productivity rates will decline.

c. Unemployment rates will decline and productivity rates will rise.

d. Unemployment and productivity rates will decline.

9. Revenue tariffs are designed to:

a. Develop new export opportunities.

b. Provide the government with tax revenues.

c. Restrict the amount of a commodity that can be imported in a given period.

d. Encourage foreign companies to limit the amount of their exports to a particular country.

10. Which of the following creates the **most** restrictive barrier to exporting to a country?

a. Tariffs

b. Quotas

c. Embargoes

d. Exchange controls

Sample Practice Questions, Answers, and Explanations

Domain 1: Governance and Business Ethics

1. Which of the following establishes a corporation's governance mechanism?

a. Stockholders

Incorrect. Stockholder's rights and obligations are described in bylaws.

b. Corporate bylaws

Correct. A corporation's governance mechanism is established by a firm's bylaws, which are a set of internal rules or policies. Bylaws describe the powers of the corporation and the duties and responsibilities of the board of directors and officers, and how to treat stockholders.

c. Board of directors

Incorrect. The board of director's duties and responsibilities are described in bylaws.

d. Corporate officers

Incorrect. Corporate officers' duties and responsibilities are described in bylaws.

2. A corporation must be managed on which of the following principles?

a. Corporate governance

Correct. For a corporation to be legitimate, its governance principles must correspond to the will of the general public. Therefore, a corporation must be managed on the principles of corporate governance defining the roles of shareholders, directors, and officers/mangers in corporate decision making and accountability. Corporate control, law, and ethics become a part of corporate governance.

b. Corporate control

Incorrect. Corporate control deals with acquiring and managing resources to operate the corporation in an efficient and effective manner.

c. Corporate law

Incorrect. Corporate laws deals with complying with laws and regulations, and knowing what are legal or illegal activities.

d. Corporate ethics

Incorrect. Corporate ethics deals with understanding what is right or good for employees and others, and knowing what are ethical or unethical activities.

3. The **major** issue embedded in the structure of modern corporations that has contributed to the corporate governance problem has been:

a. Separation of purchase from lease.

Incorrect. This is not a major issue compared to the separation of ownership from control.

b. Separation of suppliers from producers.

Incorrect. This is not a major issue compared to the separation of ownership from control.

c. Separation of ownership from control.

Correct. This is the major issue embedded in the structure of modern corporations that has contributed to the corporate governance problem. Stockholders are owners, and the board of directors, officers, and managers control the corporation on a day-to-day basis. This means no one shareholder or a group of shareholders own enough shares to exercise control; so shareholders perceive themselves to be investors rather than owners.

d. Separation of employees from independent contractors.

Incorrect. This is not a major issue compared to the separation of ownership from control.

4. Which of the following is the **major** reason for agency problems to exist?

a. Owner interest

Incorrect. This has no influence on agency problems.

b. Self-interest

Correct. Agency problems develop when the interests of the shareholders are not aligned with the interests of the manager, and the manager (who is simply a hired agent with the responsibility of representing the owner's (principal's) best interest) begins to pursue self-interest instead.

c. Community interest

Incorrect. This has no influence on agency problems

d. Corporate interest

Incorrect. This has no influence on agency problems

5. The practice of obtaining critical information from a company in faith and then using that information for one's own personal financial gain is called:

a. Financial trading.

Incorrect. This choice can result from insider trading as outcomes or tools .

b. Insider trading.

Correct. Insider trading is the practice of obtaining critical information from inside a company and then using that information for one's own personal financial gain. Insider trading perpetrated by corporate executives and managers should be prohibited and reported to the board through whistleblowing activity.

c. Shareholder trading.

Incorrect. This choice can result from insider trading as outcomes or tools.

d. Investor trading.

Incorrect. This choice can result from insider trading as outcomes or tools.

6. Which of the following is **not** an example of ethical dilemma facing a business manager involving a conflict between the:

a. Part versus whole.

Incorrect. See correct answer (d).

b. Individual versus organization.

Incorrect. See correct answer (d).

c. Organization versus society.

Incorrect. See correct answer (d).

d. Individual versus family.

Correct. Ethics deals with deciding and acting on what is right or wrong in a particular situation. Basically, ethics is concerned with knowing what is good and bad and separating them. Most ethical dilemmas involve a conflict between the needs of the part and those of the whole—the individual versus the organization or the organization versus society as a whole. The ethical dilemma between an individual and his or her family is outside of a business situation.

7. Abusive acts can be:

a. Legal but unethical.

Correct. Abuse occurs when the conduct of an activity or function falls short of expectations for prudent behavior. Abuse is distinguished from noncompliance in that abusive conditions may not directly violate laws or regulations. Abusive activities may be within the letter of the laws and regulations but violate their spirit or the more general standards of impartial behavior, and more specifically the ethical behavior. This means that abusive acts can be legal but unethical.

b. Ethical but illegal.

Incorrect. See correct answer (a).

c. Legal and ethical.

Incorrect. See correct answer (a).

d. Illegal and unethical.

Incorrect. See correct answer (a).

8. Which of the following statement is **not** true about ethics and law?

a. Ethical behavior resides above the legal behavior.

Incorrect. See correct answer (c).

b. Law embodies notions of ethics.

Incorrect. See correct answer (c).

c. Law addresses all ethical questions.

Correct. The generally accepted view of ethics is that the ethical behavior resides above the legal behavior. Note that in many respects, the law and ethics overlap because the law embodies notions of ethics. That is, the law may be seen as a reflection of what society thinks are minimal standards of conduct and behavior. It is important to note that the law does not address all realms in which ethical questions might be raised. Thus, there are clear roles for both law and ethics to play in the society. To rephrase, not all unethical actions are illegal and not all illegal actions are unethical, depending on local cultures and legal jurisdictions.

d. Law and ethics have clear roles to play in the society.

Incorrect. See correct answer (c).

9. Which type of social responsibility embraces those activities and practices that are expected or prohibited by societal members even though they are **not** codified into law?

a. Ethical responsibilities

Correct. Because laws are important but not adequate, ethical responsibilities embrace those activities and practices that are expected or prohibited by societal members even though they are not codified into law. Ethical responsibilities embody the full scope of norms, standards, and expectations that reflect a belief of what consumers, employees, shareholders, and the community regard as fair, just, and in keeping with the respect for or protection of stakeholders' moral rights. Philanthropic responsibilities include donating money and property to social programs (Archie B. Carroll, "The Four Faces of Corporate Citizenship," *Business and Society Review* 100–101 (1998): 1–7).

b. Legal responsibilities

Incorrect. Incorrect. See correct answer (a).

c. Philanthropic responsibilities

Incorrect. See correct answer (a).

d. Economic responsibilities

Incorrect. See correct answer (a).

10. Which of the following refers to the corporate behavior in response to market forces or legal constraints?

a. Social obligation.

Correct. Sethi (S. Prakash Sethi, "Dimensions of Corporate Social Performance: An Analytical Framework," *California Management Review* (Spring 1975): 58–64) proposes a three-stage schema for classifying corporate behavior in responding to social or societal needs: social obligation, social responsibility, and social responsiveness. Social obligation is corporate behavior in response to market forces or legal constraints.

b. Social responsibility

Incorrect. See correct answer (a).

c. Social responsiveness

Incorrect. See correct answer (a).

d. Social attitude

Incorrect. See correct answer (a).

Domain 2: Risk Management

1. Risk can be categorized as:

a. Objective-subjective and perils-hazards.

Incorrect. It is a partial answer.

b. Objective-subjective, physical-moral-morale, and pure-speculative.

Incorrect. It is a partial answer.

c. Static-dynamic, subjective-objective, and pure-speculative.

Correct. Risks can be classified into three types: static versus dynamic, subjective versus objective, and pure versus speculative.

d. Objective-subjective, physical-moral-morale, pure-speculative, and perils-hazards.

Incorrect. It is a partial answer. Pure risk is a condition in which there is the possibility of loss or no loss only. Peril is the cause of possible loss. Hazard is a condition that creates or increases the probability of loss .

2. The three **most** commonly used methods of loss control are:

a. Risk retention, risk avoidance, and risk transfer.

Incorrect. Risk retention, risk avoidance, and risk transfer are risk-management techniques focusing on risk financing methods. Risk avoidance is different from loss control, because the firm or individual is still engaging in operations that gave rise to particular risks.

b. Self-insurance, diversification, and risk transfer.

Incorrect. Self-insurance, diversification, and risk transfer are not loss control methods. Instead, they are risk financing methods.

c. Frequency reduction, severity reduction, and cost reduction.

Correct. Common methods of loss control include reducing the probability of losses or decreasing the cost of losses that do occur. Probability of losses is related to frequency and severity. Cost reduction is also a method of controlling losses.

d. Insurance transfers, frequency reduction, and severity reduction.

Incorrect. It mixes both correct and incorrect answers.

3. Self-insurance differs from the establishment of a reserve fund in that:

a. Establishing a reserve fund is a form of risk retention.

Incorrect. A reserve fund may not be enough for large losses.

b. Self-insurance involves prefunding of expected losses through a fund specifically designed for that purpose.

Incorrect. This it is a necessary element of self-insurance.

c. Self-insurance requires the existence of a group of exposure units large enough to allow accurate loss prediction.

Correct. Self-insurance by a firm is possible and feasible when it has accurate records or has access to satisfactory statistics to enable it to make good estimate of expected losses. The general financial condition of the firm should be satisfactory and the firm's management must be willing and able to deal with large and unusual losses.

d. Self-insurance requires the formation of a subsidiary company.

Incorrect. Self-insurance does not require the creation of a subsidiary company.

4. The purchase of insurance is a common form of:

a. Risk retention.

Incorrect. Risk retention is a technique for managing risk and does not involve insurance.

b. Risk transfer.

Correct. The most widely used form of risk transfer is insurance.

c. Risk avoidance.

Incorrect. Risk avoidance is best if it can be done and does not involve insurance.

d. Loss control.

Incorrect. Loss control involves risk reduction or risk mitigation and does not involve insurance.

5. Which of the following **best** represents the fit-gap analysis as a risk management tool?

a. This analysis determines the difference between the actual outcome and the expected outcome.

Correct. This choice compares the actual outcomes and expected outcomes and determines whether these outcomes fit with each other or any gap left between them.

b. This analysis is used for managing uncertainty as it may be subdivided into sequential decision analysis and irreversible investment theory.

Incorrect. This choice defines option analysis.

c. This analysis deals with quantitative data in terms of dollars and ratios.

Incorrect. This choice defines economic analysis (e.g., return on investment, net present value, internal rate of return, return on sales, and return on equity).

d. This analysis involves assigning weights to responses to questions addressing areas that may introduce elements of risk.

Incorrect. This choice defines subjective scoring analysis.

6. Which of the following financial and accounting practices is **not** a risk for public corporations?

a. Financial engineering.

Correct. The scope of financial engineering involves creating new financial instruments (e.g., derivative securities) or combining existing derivatives to accomplish specific hedging goals (i.e., to reduce financial risk).

b. Earnings management

Incorrect. This is a risk to a public corporation.

c. Creative accounting

Incorrect. This is a risk to a public corporation.

d. Off-the-books accounts

Incorrect. This is a risk to a public corporation.

7. Which of the following has been determined to be a **reasonable** level of risk?

a. Minimum risk

Incorrect. Minimum risk is the reduction in the total risk that results from the impact of in-place safeguards or controls.

b. Acceptable risk

Correct. Acceptable risk is the level of residual risk that has been determined to be a reasonable level of potential loss or disruption for a specific computer system.

c. Residual risk

Incorrect. Residual risk results from the occurrence of an adverse event after adjusting for the impact of all safeguards in place.

d. Total risk

Incorrect. Total risk is the potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit system vulnerability).

8. Which of the following enterprise risk management (ERM) frameworks address market risk?

a. Strategic risks

Incorrect. Strategic risks include political risk, regulatory risk, reputation risk, leadership risk, and market brand risk.

b. Operational risks

Incorrect. Operational risks include an organization's systems, technology, and people.

c. Financial risks

Correct. Financial risk includes risks from volatility in foreign currencies, interest rates, and commodities. It also includes credit risk, liquidity risk, and market risk.

d. Hazard risks

Incorrect. Hazard risks include natural disasters, impairment of physical assets, and terrorism.

9. The scope of enterprise risk management (ERM) should encompass which of the following?

I. Hazards
II. Opportunities
III. Strengths
IV. Weaknesses

a. I only

Incorrect. See correct answer (c).

b. II only

Incorrect. See correct answer (c).

c. I and II.

Correct. It is important to emphasize that the uncertainties could have a potential upside or downside so that the scope of ERM encompasses the more traditional view of potential hazards as well as opportunities. Hazard risks include both insurable and uninsurable risks.

d. III and IV

Incorrect. See correct answer (c).

10. Which of the following is **best** to manage the enterprise-wide risk management program?

a. Chief risk officer

Incorrect. See correct answer (b).

b. Board of directors

Correct. Risk is pervasive throughout an organization as it can arise from any business function or process at any time without warning. Because of this widespread exposure, no single functional department management, other than the board of directors, can oversee the enterprise-wide risk management program. This approach also supports the idea that risks cannot be identified, measured, and monitored on a piecemeal basis. A holistic approach is needed.

c. Chief financial officer

Incorrect. See correct answer (b).

d. Chief governance officer

Incorrect. See correct answer (b).

Domain 3 Organizational Structure, Business Processes, and Risks

1. The relationship between organizational structure and technology suggests that in an organization using mass production technology (e.g., automobile manufacturing), the **best** structure would be:

a. Organic, emphasizing loose controls and flexibility.

Incorrect. Mass production technology should not be matched with an organic structure.

b. Matrix, in which individuals report to both product and functional area managers.

Incorrect. Matrix is not a type of structure but rather a type of departmentalization and should not be used with mass production.

c. Mechanistic, that is, highly formalized, with tight controls.

Correct. Mass production would be best matched with a mechanistic, highly formalized structure.

d. Integrated, emphasizing cooperation among departments.

Incorrect. There is no such thing as integrated structure, and integration is not conducive to mass production.

2. Routine tasks, which have few exceptions and problems that are easy to analyze, are conducive to:

a. Formalized structure, where procedure manuals and job descriptions are common.

Correct. Routine tasks are conducive to formalized structure.

b. Decentralized decision making, where decisions are pushed downward in the organization.

Incorrect. Routine tasks are conducive to centralization.

c. Organic structures that emphasize adaptability and flexibility to changing circumstances.

Incorrect. Routine tasks are conducive to mechanistic, not organic, structures.

d. High degrees of job satisfaction on the part of employees performing them.

Incorrect. Job satisfaction is often low in tasks that are routine and repetitive.

3. Which of the following theories predicts that employee behavior depends on the belief that good performance will be rewarded by continued employment?

a. Equity theory: Employees compare their job inputs and outcomes with those of others and then react to eliminate inequities.

Incorrect. In equity theory, the employees compare their job inputs and outcomes with others and then respond to eliminate inequities.

b. Expectation theory: The strength of a tendency to act in a certain way depends on the strength of an expectation that an act will be followed by a given outcome.

Correct. The strength of a tendency to act in a certain way depends on the strength of an expectation that an act will be followed by a given outcome.

c. Goal-setting theory: Specific and difficult goals lead to higher performance.

Incorrect. Goal-setting theory postulates that specific and difficult goals lead to higher performance.

d. Reinforcement theory: Behavior is a function of its consequences.

Incorrect. Reinforcement theory states that behavior is a function of its consequences.

4. Which of the following has a flat organizational structure compared to others?

a. Organization A with 11 hierarchical levels

Incorrect. See correct answer (b).

b. Organization B with 3 hierarchical levels

Correct. A flat structure has a wide span, is horizontally dispersed, and has fewer hierarchical levels. Relative to a flat structure, a tall structure has a narrow span of management and more hierarchical levels.

c. Organization C with 8 hierarchical levels

Incorrect. See correct answer (b).

d. Organization D with 6 hierarchical levels

Incorrect. See correct answer (b).

5. The most fundamental flaw of cost-plus pricing is that it:

a. Fails to account for competition.

Incorrect. See correct answer (b).

b. Ignores demand.

Correct. Price reflects some unit of value given up by one party in return for something from another party. The setting price based on costs has become a common practice. Two approaches include standard markup pricing and target return pricing. Cost-plus pricing method ignores demand since costs are generated internally and since the demand is created externally to an organization.

c. Ignores industry-wide standard markup policies.

Incorrect. See correct answer (b).

d. Places too much emphasis on competition.

Incorrect. See correct answer (b).

6. "Selling price = Unit cost + Desired profit" represents which of the following pricing approaches?

a. Profit maximization

Incorrect. See correct answer (c).

b. Demand-based pricing

Incorrect. See correct answer (c).

c. Target return pricing

Correct. Two pricing approaches based on cost include standard markup pricing and target return pricing. Target return pricing adds both cost per unit and desired profit and is calculated as: Selling price per unit = Unit cost per unit + Desired profit per unit. A standard markup percentage based on management profit goal is added to the cost in the standard markup pricing approach.

d. Standard markup

Incorrect. See correct answer (c).

7. Choosing vendors based solely on which of the following factors is detrimental to the long-term success of a buying firm?

a. Quality

Incorrect. See correct answer (c).

b. Service

Incorrect. See correct answer (c).

c. Price

Correct. Suppliers should be viewed as outside partners who can contribute to the long-term success of a buying firm. If suppliers are selected on price only, they will be switched continuously, which will destabilize the purchasing process.

d. Delivery

Incorrect. See correct answer (c).

8. Supplier audits are an important first step in:

a. Supplier certification.

Correct. Supplier audits are an important first step in the supplier certification program.

b. Supplier relationships.

Incorrect. This choice occurs after supplier certification.

c. Supplier partnerships.

Incorrect. This choice occurs after supplier certification.

d. Strategic partnerships.

Incorrect. This choice occurs after supplier certification.

9. Customers in which of the following phases of the product life cycle are called laggards?

a. Introduction

Incorrect. See correct answer (d).

b. Growth

Incorrect. See correct answer (d).

c. Maturity

Incorrect. See correct answer (d).

d. Decline

Correct. Innovators and early adopters are those customers who are willing to take more risk and buy the product shortly after introduction. During the growth phase, product purchase begins to spread to the early majority of the mass market, with full penetration and adoption by the late majority occurring primarily in the maturity phase. Near the product's decline, only laggards are left purchasing the product.

10. Few competitors exist in which phase of the product life cycle?

a. Introduction

Correct. In the introduction phase of the product life cycle, few competitors exist. A growing number exists in the growth phase, many rivals exist in the maturity phase, and declining number exists in the decline phase. Similarly, negative cash flow occurs in the introduction phase, is moderate in the growth phase, is high in the maturity stage, and is low in the decline phase.

b. Growth

Incorrect. See correct answer (a).

c. Maturity

Incorrect. See correct answer (a).

d. Decline

Incorrect. See correct answer (a).

11. Regarding the theory of constraints in operations, which of the following does **not** describe a bottleneck situation appropriately?

a. A machine exists where jobs are processed at a slower rate than they are demanded.

Incorrect. See correct answer (c).

b. A work center exists where jobs are processed at a slower rate than they are demanded.

Incorrect. See correct answer (c).

c. An employee's skill levels are more than needed for a specific job but less than needed for any general job.

Correct. A bottleneck is a constraint in a facility, function, department, or resource whose capacity is less than the demand placed on it. For example, a bottleneck machine or work center exists (1) where jobs are processed at a slower rate than they are demanded and (2) where the demand for a company's product exceeds the ability to produce the product. Generally, bottlenecks deal with products, not people. For example, an employee's skill levels are more than needed for a specific job but less than needed for any general job is related to people .

d. The demand for a company's product exceeds its ability to produce that product.

Incorrect. See correct answer (c).

12. Regarding production process flows, which of the following is **not** a part of the levers for managing throughput of a process?

a. Decrease resource idleness

Incorrect. This choice is an example of a lever in managing the throughput.

b. Increase effective capacity

Incorrect. This choice is an example of a lever in managing the throughput.

c. Reduce setup resources

Incorrect. This choice is an example of a lever in managing the throughput.

d. Decrease theoretical capacity

Correct. Three operational process flow measures include flow time, inventory, and throughput. Theoretical capacity should not be decreased; instead, it should be increased by decreasing the unit load on the bottleneck resource pool.

13. Which of the following inventory items would be the **most** frequently reviewed in an ABC inventory control system?

a. Expensive, frequently used, high stock-out cost items with short lead times

Incorrect. Long, not short, lead times prompt a more frequent review in the ABC inventory control system.

b. Expensive, frequently used, low stock-out cost items with long lead times

Incorrect. High, not low, stock-out costs prompt a more frequent review in an ABC inventory control system.

c. Inexpensive, frequently used, high stock-out cost items with long lead times

Incorrect. Expensive, not inexpensive, items prompt a more frequent review in an ABC inventory control system.

d. Expensive, frequently used, high stock-out cost items with long lead times

Correct. All of these items prompt a more frequent review in an ABC inventory control system.

14. What are the three factors a manager should consider in controlling stock-outs?

a. Holding costs, quality costs, and physical inventories

Incorrect. These are inventory-related terms but none will controls stock-outs.

b. Economic order quantity, annual demand, and quality costs

Incorrect. The order quantity and annual demand are not factors in the stock-out problem.

c. Time needed for delivery, rate of inventory usage, and safety stock

Correct. Delivery time, usage rate, and level of safety stock are all considerations in controlling stock-outs.

d. Economic order quantity, production bottlenecks, and safety stock

Incorrect. Production bottlenecks are the results of a stock-out; they are not a method of control. Also, economic order quantity is irrelevant to stock-outs.

15. Reordering of specific items from vendors should be based on:

a. Computations on the basis of economic order quantities.

Correct. Computations on the basis of economic order quantities (EOQs) will minimize the EOQ objective, but EOQ assumes stationary demand, which is not the case here.

b. Demand forecasting based on early orders for the items.

Correct. A stated requirement is demand forecasting based on early orders for items, which means that company personnel have learned that the best predictor of subsequent sales of a specific item is sales in the first few days after it has been made available.

c. Market demographics.

Incorrect. This is not the critical ordering factor for a specific item.

d. Vendor quantity discounts and warehouse space.

Incorrect. Vendor quantity discounts and warehouse space are valid considerations only if the company would order the item in those quantities anyway.

16. A risk associated with just-in-time (JIT) production is the:

a. Increased potential for early obsolescence of inventories of finished goods.

Incorrect. To the contrary, finished goods inventories are virtually eliminated.

b. High cost of material handling equipment.

Incorrect. JIT does not necessarily require high-cost material handling equipment.

c. Potential for significant costs associated with reworking defective components.

Incorrect. If a defect is discovered, production is stopped.

d. Critical dependency on a few vendors.

Correct. Because materials are delivered as needed, it is imperative to establish and maintain good relations with those critical suppliers.

17. With regard to inventory management, an increase in the frequency of ordering will normally:

a. Reduce the total ordering costs.

Incorrect. Total ordering costs would increase.

b. Have no impact on total ordering costs.

Incorrect. total ordering costs would increase.

c. Reduce total carrying costs.

Correct. As the frequency of ordering increases, total carrying costs are reduced by the average that inventory level is reduced.

d. Have no impact of total carrying costs.

Incorrect. Total carrying costs are reduced.

18. Which of the following represents an integration of diverse technologies such as point-of-sale terminals, personal identification numbers, and automated teller machines?

a. Electronic data interchange systems

Incorrect. An electronic data interchange (EDI) system represents the electronic transfer of specially formatted standard business documents (e.g., purchase orders, shipment instructions, invoices, payments, and confirmations) sent between business partners. EDI offers the ability to develop closer relationships between the buyers and sellers. EDI is a direct computer-to-computer exchange between two organizations, and it can use either a value-added network (VAN-EDI) or the Internet (Web-EDI) with XML standards. EDI does not use or integrate point-of-sale terminals, personal identification numbers, and automated teller machines because it deals with business-oriented transactions, not consumer-oriented transactions.

b. Electronic funds transfer systems

Correct. In electronic funds transfer (EFT) systems, money and other financial information is transferred electronically from one institution to another through the Internet. For example, (1) banks can transfer money from an account in one bank to another account in another bank, (2) government can deposit benefits directly into recipients' bank accounts, and (3) consumers can pay their bills electronically from banks to credit card companies and others. During these financial transactions, EFT requires the use or integration of point-of-sale terminals, personal identification numbers, and automated teller machines because EFT deals with consumer-oriented transactions, not business-oriented transactions.

c. Intranet systems

Incorrect. An intranet is an internal network within an organization to facilitate employee communications and information sharing. Organizations are posting information to their internal Web sites and using Web browsers as a common collaborative tool. An example of an intranet application is a customer database accessible via the Web. Sales staff could use this database to contact customers about new product offerings and send them quotes. Other applications include internal phone books, procedures manuals, training manuals, and purchase requisition forms. The intranet does not use or integrate point-of-sale terminals, personal identification numbers, and automated teller machines because it deals with business-oriented transactions, not consumer-oriented transactions.

d. Extranet systems

Incorrect. The scope of extranet includes vendor or customer organizations that do business with the suppler organization. Extranets are intranet-based networks restricted to select audiences, such as vendors, clients, and other interested parties outside the organization. The extranet does not use or integrate point-of-sale terminals, personal identification numbers, and automated teller machines because it deals with business-oriented transactions, not consumer-oriented transactions.

19. Stock brokers/dealers and stock markets employ which of the following electronic commerce models?

a. Consumer-to-business (C2B)

Incorrect. The C2B e-commerce model deals mostly with individual consumers and some businesses request lower prices for airline tickets, hotels, car rentals, vacations, and resorts, and businesses come back with the lowest price.

b. Business-to-consumer (B2C)

Incorrect. The B2C e-commerce model involves online retail stores selling goods directly to consumers.

c. Business-to-business (B2B)

Incorrect. The B2B e-commerce model involves Internet enabling of existing relationships between two companies in exchanging goods and services (e.g., electronic data interchange).

d. Exchange-to-exchange (E2E)

Correct. In the E2E e-commerce model, the electronic exchanges formally connect to one another for the purpose of exchanging information. Examples include stock brokers/dealers with stock markets and vice versa.

20. In which of the following phases of business development life cycle will both outputs and employment be declining?

a. Peak

Incorrect. See correct answer (b).

b. Recession

Correct. Economists suggest four phases of the business cycle: peak, recession, trough, and recovery. During the recession phase, both output and employment will decline, but prices tend to be relatively inflexible in a downward direction.

c. Trough

Incorrect. See correct answer (b).

d. Recovery

Incorrect. See correct answer (b).

21. In business activity, both seasonal variations and secular trends are due to which of the following?

a. Cyclical fluctuations

Incorrect. See correct answer (b).

b. Noncyclical fluctuations

Correct. Both seasonal variations and secular trends are due to noncyclical fluctuations. Many businesses, such as retail, automobile, construction, and agriculture, are subject to seasonal variations such as pre-Christmas and pre-Easter holidays. Business activity is also subject to a secular trend. The secular trend of an economy is its expansion or contraction over a long period of time (i.e., 25 or more years).

c. Business expansions

Incorrect. See correct answer (b).

d. Business contractions

Incorrect. See correct answer (b).

22. The ISO 14000 standard focuses on environmental management system and the ISO 14001 standard focuses on the framework for implementing environmental strategies. Which of the following is the scope of the ISO 14001 standard?

a. Minimize waste in products.

Incorrect. See correct answer (c).

b. Minimize redesign of products.

Incorrect. See correct answer (c).

c. Conduct environmental audit.

Correct. Conducting an environmental audit is part of the scope of the ISO 14001 standard. The ISO 14001 framework includes a policy, a planning process, an organizational structure, specific objectives and targets, specific implementation programs, communication and training programs, and management review, monitoring, and corrective action, which addresses environmental audit.

The other three choices are part of the scope of the ISO 14000 standard. The scope of that standard includes all efforts to minimize waste and redesign manufacturing processes, products, and packaging to prevent pollution. More attention should be given to pollution prevention than correction.

d. Prevent pollution.

Incorrect. See correct answer (c).

23. The ISO 22301 standard focuses on which of the following subjects?

a. Business continuity management systems and requirements

Correct. The ISO 22301 standard focuses on business continuity management systems and requirements in order to prepare for, to protect against, and to reduce the likelihood of occurrence of disasters or disruptive incidents (i.e., man-made or natural). The goal is to respond to and recover from disasters and incidents and to improve business continuity capabilities and operations.

b. System and software life cycles

Incorrect. ISO 15026 addresses software assurance in terms of managing risks and assuring safety, security, and dependability within the context of system and software life cycles.

c. Code of practice for information security management

Incorrect. ISO 17799 (later changed to 27002) addresses information technology security techniques and code practice for information security management.

d. Independent software testing

Incorrect. ISO 17025 addresses independent testing of software using either white box or black box testing methods.

24. Which of the following scope items for an outsourced vendor takes on a significant dimension in a supply-chain environment?

a. Liabilities and guarantees

Correct. In a supply-chain environment, there could be several suppliers and integrators in developing or delivering a specific product or service to a user customer or client. Liabilities and guarantees take on a significant dimension in order to pin down each party's roles, responsibilities, liabilities, guarantees, and remedies to problems encountered. The other three choices are also important.

b. Well-defined service levels

Incorrect. See correct answer (a).

c. Licensing of services and products

Incorrect. See correct answer (a).

d. Changes to terms and conditions of services

Incorrect. See correct answer (a).

25. When managing a third-party organization such as an outsourcing vendor, which of the following is **not** applicable?

a. Due diligence review

Incorrect. This choice is applicable to outsourcing vendors.

b. Rules of engagement

Incorrect. This choice is applicable to outsourcing vendors.

c. Rules of behavior

Correct. The rules of behavior document is applicable to internal employees of an organization, not for external, third-party organizations.

d. Contractual agreement

Incorrect. This choice is applicable to outsourcing vendors.

Domain 4: Communication

1. Which of the following enables communicators to know if their message has been understood?

a. Encoding

Incorrect. See correct answer (c).

b. Decoding

Incorrect. See correct answer (c).

c. Feedback

Correct. Either verbal or nonverbal feedback from the receiver to the sender is required to complete the communication process. Without this feedback, senders have no way of knowing whether their ideas or messages have been accurately understood. Sender, encoding, medium, decoding, receiver, and feedback are part of the basic communication process. Encoding translates thoughts into words. Successful decoding is more likely to occur if the receiver knows the language and terminology used in the message.

d. Perception

Incorrect. See correct answer (c).

2. Which of the following refers to the unofficial and informal communication system in an organization?

a. Grapevine

Correct. Water fountain talks, hallway gossiping, and cafeteria chatting are all part of the grapevine. Cluster is the most common grapevine pattern.

b. Water fountain talks

Incorrect. See correct answer (a).

c. Hallway gossiping

Incorrect. See correct answer (a).

d. Cafeteria chatting

Incorrect. See correct answer (a).

3. Most managers have which one of the following attitudes toward the grapevine?

a. Positive

Incorrect. See correct answer (c).

b. Uncertain

Incorrect. See correct answer (c).

c. Negative

Correct. About 75% of grapevine rumors are accurate, and most managers have a negative attitude about the grapevine.

d. Neutral

Incorrect. See correct answer (c).

4. Communication channel richness refers to which of the following?

a. Number of messages a channel can carry at one time

Incorrect. See correct answer (c).

b. Speed in which messages can be carried

Incorrect. See correct answer (c).

c. Amount of information that can be transmitted during a communication episode

Correct. Channel richness refers to the amount of information that can be transmitted during a communication episode.

d. Number of channels available at any one time

Incorrect. See correct answer (c).

5. Which of the following is the **richest** medium for communication?

a. Telephone conversations

Incorrect. See correct answer (b).

b. Face-to-face discussions

Correct. Face-to-face discussion is the richest medium because it permits direct experience, multiple information cues, immediate feedback, and personal focus. Impersonal written media, including flyers, bulletins, and standard computer reports, are the lowest in richness. These channels are not focused on a single receiver, use limited information cues, and do not permit feedback.

c. Electronic media

Incorrect. See correct answer (b).

d. Written media

Incorrect. See correct answer (b).

6. When dealing with employees, which of the following is **not** an example of possible management's negative actions if whistleblowing employees report misconduct of management?

a. Reduced duties

Incorrect. See correct answer (b).

b. Coercion of political activity

Correct. Coercion of political activity is one of the prohibited personnel practices. The other three choices are examples of management's negative actions if whistleblowing employees report misconduct of management.

c. Reassignment of work location

Incorrect. See correct answer (b).

d. Reshuffling of work schedules

Incorrect. See correct answer (b).

7. Which of the following was **not** a major shareholder initiative?

a. Rise of shareholder activist groups

Incorrect. The rise of shareholder activist groups is a major initiative to express shareholders' concerns about how a corporation operates.

b. Shareholder-initiated golden parachutes

Correct. Shareholders do not initiate golden parachutes; management does. A golden parachute is a contract in which a corporation agrees to make payments to key management and senior officers in the event of a change in the control of the corporation.

c. Shareholder resolutions and annual meetings

Incorrect. The filing of shareholder resolutions and activism at annual meetings is a major initiative to document the shareholders' issues raised and solutions reached.

d. Shareholder lawsuits

Incorrect. The filing of shareholder lawsuits is becoming common to express the shareholders' disappointment and frustration with the management of the corporation.

8. When dealing with stakeholders, which of the following ethical and legal principles is **not** applicable?

a. Due process

Incorrect. The due process principle applies to stakeholders, who are owners, investors, and employees. Due process means following rules and principles so that an individual is treated fairly and uniformly at all times with basic rights protected (e.g., life, liberty, and property). It also means fair and equitable treatment to all concerned parties so that no person is deprived of life, liberty, or property without due process of the law, which is the right to notice and a hearing. Due process requires due care and due diligence in fulfilling the right to notice and for a fair hearing.

b. Due diligence

Incorrect. The due diligence principle applies to stakeholders, who are owners, investors, and employees. Due diligence requires organizations to develop and implement an effective system of controls, policies, and procedures to prevent and detect violation of policies and laws.

c. Due care

Incorrect. The due care principle applies to stakeholders, who are owners, investors, and employees. Due care means reasonable care that promotes the common good. It is maintaining minimal and customary practices

d. Duty of loyalty

Correct. Duty of loyalty is expected of board of directors and officers of a corporation in that they have a duty not to act adversely to the interests of the corporation and not to subordinate their personal interests to those of the corporation and its shareholders. Therefore, duty of loyalty does not apply to stakeholders.

9. Which of the following is the **ultimate** goal of shareholder and investor communications?

a. Honesty

Correct. Honesty of management is the ultimate goal of shareholder and investor communications, although the communication should provide consistency, clarity, candor, and effectiveness. Corporations should consider candor, need for timely disclosure, and effective use of technology. However, the ultimate goal of shareholder and investor communications is honest, intelligible, meaningful, and timely and broadly disseminated information.

b. Consistency

Incorrect. See correct answer (a).

c. Clarity

Incorrect. See correct answer (a).

d. Effectiveness

Incorrect. See correct answer (a).

10. When handling related parties, which of the following is the **most** difficult type of transaction?

a. Misreported sales between affiliates

Incorrect. This choice is an example of related party normal transactions.

b. Unspecified intercompany transactions

Incorrect. This choice is an example of related party normal transactions.

c. Personal loans to the current chief executive

Incorrect. This choice is an example of related party normal transactions.

d. A close family who is a major shareholder

Correct. Transactions involving major shareholders (e.g., close family and relations), either directly or indirectly, are potentially the most difficult type of transactions.

Domain 5: Management and Leadership Principles

1. Where does the information about opportunities and threats come from for a company?

a. An analysis of the organization's internal environment

Incorrect. See correct answer (c).

b. A department-by-department study of the organization

Incorrect. See correct answer (c).

c. A scan of the external environments

Correct. While information about strengths and weaknesses of organization come from internal sources, information about opportunities and threats will come from external sources. The external sources can include competition, government, economy, and political, legal, demographic, and cultural changes.

d. An analysis of employee grievances

Incorrect. See correct answer (c).

2. The costs of providing training and technical support to the supplier in order to increase the quality of purchased materials are examples of:

a. Prevention costs.

Correct. Prevention costs are costs incurred to prevent defects from occurring during the design and delivery of products or services. Prevention costs can keep both appraisal and failure costs to a minimum.

b. Appraisal costs.

Incorrect. Appraisal costs are associated with measuring, evaluating, or auditing products to assure conformance with quality standards and performance requirements.

c. Internal failure costs.

Incorrect. Failure costs are two types (i.e., internal and external) and are associated with evaluating and either correcting or replacing defective products, components, or materials that do not met quality standards. Internal failure costs occur prior to the completion, or shipment of a product or rendering of a service to a customer, which will increase repair, redesign, or rework.

d. External failure costs.

Incorrect. Failure costs are two types (i.e., internal and external) and are associated with evaluating and either correcting or replacing defective products, components, or materials that do not met quality standards. External failure costs occur after a product is shipped or a service is rendered, which will increase product warranty charges and returns costs.

3. All of the following are effective ways to prevent service mistakes from occurring **except**:

a. Source inspections.

Incorrect. See correct answer (d).

b. Self-inspections.

Incorrect. See correct answer (d).

c. Sequence checks.

Incorrect. See correct answer (d).

d. Mass inspections.

Correct. Mistake-proofing (also called idiot proofing or poka-yoke) a service requires identifying when and where failures occur. Once a failure is identified, the source must be found. The final step is to prevent the mistake occurring through source inspections, self-inspections, or sequence checks. Mass or final inspections are expensive, time consuming, and ineffective as it is too late in the game to make changes.

4. Which of the following is **not** one of the principles of total quality management (TQM)?

a. Do it right the first time.

Incorrect. This is a principle of TQM.

b. Strive for zero defects.

Correct. Striving for zero defects is not one of the principles of TQM but is a principle of Six Sigma approaches. Striving for zero defects is the goal of manufacturing management achieved through statistical process control and Six Sigma methodologies, which are subsets of TQM.

c. Be customer centered.

Incorrect. This is a principle of TQM.

d. Build teamwork and empowerment.

Incorrect. This is a principle of TQM.

5. Recent events caused the time series used by an electric utility to become too unpredictable for practical use. As a result, the utility developed a model to predict the demand for electricity based on factors such as class of service, population growth, and unemployment in the area of service. The discipline that deals with such models is called:

a. Linear programming.

Incorrect. Linear programming is a problem-solving approach developed for situations involving maximizing or minimizing a linear function based on certain linear constraints.

b. Network analysis.

Incorrect. Network analysis is used to solve management problems in areas such as system design and project scheduling.

c. Operations research.

Incorrect. Operations research is a term used interchangeably with management science, an approach to managerial decision making based on scientific methods and extensive use of quantitative analysis.

d. Econometrics.

Correct. Econometrics is a forecasting model that uses a number of economic and demographic time series.

6. A company wishes to forecast from time series data covering 20 periods. Which of the following is **not** an appropriate forecasting technique?

a. Weighted least squares

Incorrect. Weighted least squares is used only in regression models that have the specification problem heteroscedasticity.

b. Exponential smoothing

Incorrect. The exponential smoothing technique (single parameter) is appropriate for such a database.

c. Delphi technique

Correct. The Delphi technique is a qualitative technique, not a quantitative technique. It is a technique used to avoid groupthink. Group members do not meet face to face to make decisions. Rather, each group member independently and anonymously writes down suggestions and submits comments, which are then centrally compiled. The compiled results are then distributed to the group members who, independently and anonymously, write additional comments. These comments are again centrally compiled and the process repeated until consensus is obtained. The Delphi technique is a group decision-making method.

d. Moving average process

Incorrect. The moving average process is used to decompose the time series components.

7. The auditor has recognized that a problem exists because the organizational unit has been too narrow in its definition of goals. The goals of the unit focus on profits, but the overall organizational goals are much broader. The auditor also recognizes that the auditee will resist any recommendations about adopting broader goals. The best course of action would be to:

a. Avoid conflict and present only those goals that are consistent with the auditee's views since all others will be ignored.

Incorrect. Organizations cannot avoid conflict. It is now becoming accepted that some levels of conflict are necessary in order for organizations to grow and adapt to a changing environment.

b. Identify the broader organizational goals and present a set of recommendations that attempts to meet both the organizational and auditee goals.

Correct. The auditor is responsible to the organization, not just the auditee, and should therefore report the problem to the auditee.

c. Subtly mix the suggested solution with the problem definition so that the auditee will identify the solution apparently independently of the auditor.

Incorrect. Mixing solutions with problem identification is a frequent problem cited in the managerial literature, but is not an effective means of dealing with the problem identified.

d. Only report the conditions found and leave the rest of the analysis to the auditees.

Incorrect. This would be a violation of the *Standards,* which specify reporting criteria.

8. Which of the following problem-solving tools is an idea-generating and consensus-building technique?

a. Brainstorming

Incorrect. Brainstorming is a technique to generate a great number of ideas.

b. Synectics

Incorrect. Synectics involves the use of nontraditional activities, such as excursions, fantasies, and analogies.

c. Systems analysis

Incorrect. Systems analysis breaks down a large problem into many smaller problems.

d. Nominal group technique

Correct. The nominal group technique is an idea-generating and consensus-building problem-solving tool. This technique gives everyone an opportunity to express ideas without being interrupted by others in the group.

9. Job performance is best defined as follows:

a. Job performance = Motivation × Ability.

Correct. Job performance is motivation multiplied by ability. The reason for the multiplication sign in the equation is because motivation cannot compensate for lack of ability. In addition to ability, skill, experience, and training are needed.

b. Job performance = Needs × Skills.

Incorrect. See correct answer (a).

c. Job performance = Satisfaction × Job experience.

Incorrect. See correct answer (a).

d. Job performance = Goals × Training.

Incorrect. See correct answer (a).

10. Individual commitment to groups is based on attractiveness and which of the following?

a. Groupthink

Incorrect. Groupthink is related to norms and describes situations in which group pressures for conformity deter the group from critically appraising unusual, minority, or unpopular views.

b. Appearance

Incorrect. Appearance is an external look of each group member in the way they see each other.

c. Cohesiveness

Correct. Individual commitment to either an informal or a formal group is based on two factors: attractiveness and cohesiveness.

d. Conformity

Incorrect. Conformity is going along or getting along with each group member.

11. "Apple polishing" is done to:

a. Make the supervisor look good.

Correct. Apple polishing is a political strategy prompted by a desire to favorably influence those who control one's career. Its major purpose is to make the supervisor look good.

b. Build an empire.

Incorrect. This is not the purpose of apple polishing.

c. Create cliques.

Incorrect. This is not the purpose of apple polishing.

d. Create destructive competition.

Incorrect. This is not the purpose of apple polishing.

12. Which of the following is a **critical** challenge in implementing employee empowerment principle?

a. Pushing authority downward closer to front-line employees

Incorrect. This is not a critical challenge.

b. Expecting accountability from all employees

Incorrect. This is not a critical challenge.

c. Delegating employees with restrictions to achieve objectives

Correct. A critical challenge in implementing employee empowerment principle is to delegate only to the extent required to achieve objectives. This requires ensuring that risk acceptance is based on sound practices for identification and minimization of risk, including sizing risks and weighing potential losses versus gains in arriving at good business decisions. This is a balancing act among risk, competence, and objectives.

The employee empowerment principle includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. It involves the degree to which individuals and teams are encouraged to use initiative in addressing issues and solving problems, as well as limits of their authority. It also deals with policies describing appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. Specifically, employee empowerment also includes pushing authority downward closer to front-line employees (choice a), expecting accountability from all employees (choice b), and developing clear and complete job description for employees (choice d), but these are not critical challenges.

d. Developing clear and complete job descriptions for employees

Incorrect. This is not a critical challenge.

13. In light of rapidly changing technologies and increasing competition and to provide the ability to affect quality initiatives, which of the following human resources policies and practices is **not** enough?

a. Hiring competent employees

Incorrect. See correct answer (b).

b. Providing one-time training for employees

Correct. It is essential that employees be equipped for new challenges as issues that enterprises face change and become more complex—driven in part by rapidly changing technologies and increasing competition. Education and training, whether classroom instructions, self-study, or on-the-job training, must prepare an entity's people to keep pace and deal effectively with the evolving environment. They will also strengthen the entity's ability to affect quality initiatives. Hiring of competent people and one-time training are not enough. The education and training process must be ongoing and continuing.

c. Encouraging continuing education for employees

Incorrect. See correct answer (b).

d. Conducting periodic performance evaluations for employees

Incorrect. See correct answer (b).

14. From a human resources policies and practices viewpoint, which of the following sends a strong message to all interested parties?

a. Expected levels of integrity

Incorrect. See correct answer (b).

b. Expected levels of disciplinary actions

Correct. Human resources practices send messages to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. Of the most, disciplinary actions send a strong message that violations of expected behavior will not be tolerated.

c. Expected levels of ethical behavior

Incorrect. See correct answer (b).

d. Expected levels of competence and trust

Incorrect. See correct answer (b).

15. Commitment falls under which of the following types of a leader's power?

a. Reward power

Incorrect. Reward power is gaining compliance through rewards.

b. Coercive power

Incorrect. Coercive power is gaining compliance through fear or threat of punishment.

c. Expert power

Incorrect. Expert power is based on the ability to dispense valued information. An example of expert power is when a financial planner manages and advises an investment portfolio for a client.

d. Referent power

Correct. Referent power comes from a leader's personality characteristics that command subordinates' identification, respect, admiration, and charisma. It is expressed through commitment.

16. Which of the following should be done **before** job descriptions are developed?

a. Job analyses

Correct. Job analysis identifies basic task and skill requirements through observation. and it should be done before job descriptions are developed.

b. Job rotation

Incorrect. Job rotation involves moving employees between various duties either inside or outside of the department they work in.

c. Job specifications

Incorrect. Job specifications or descriptions outline the role expectations and skill requirements for a specific job.

d. Job matrix

Incorrect. A job matrix shows where individual employees fit with what jobs or positions, which is an example of fit-gap analysis.

17. Which of the following defines the process of evaluating an individual's contribution as a basis for making objective personnel decisions?

a. Performance appraisal

Correct. Performance appraisal defines the process of evaluating an individual's contribution as a basis for making objective personnel decisions.

b. Environmental factors

Incorrect. Environmental factors include intrinsic and extrinsic rewards.

c. Facilitation skills

Incorrect. Facilitation skills include diplomacy, negotiating, and communicating skills.

d. Training and development

Incorrect. Training and development is a part of making an employee learn new skills for career advancement.

18. Negotiation, manipulation, coercion, employee education, and increased communication are all ways in which managers can:

a. Improve employee morale.

Incorrect. All five items listed may either increase or decrease morale.

b. Overcome resistance to change.

Correct. The five items listed in the question are generally recommended as means of overcoming resistance to change. Each technique is recommended in different situations and is likely to address specific resistance to change factors.

c. Maintain control of information.

Incorrect. All five items listed may either increase or decrease a manager's control over information or the organization.

d. Demonstrate their power to both their supervisors and subordinates.

Incorrect. Although use of manipulation and coercion may help a manager demonstrate power, education, communication, and negotiation would not.

19. The adoption of a new idea or behavior by an organization is known as organizational

a. Development.

Incorrect. Organizational development is planned change programs intended to help people and organization function more effectively.

b. Change.

Correct. Organizational change is defined as the adoption of a new idea or behavior by an organization.

c. Structure.

Incorrect. Organizational structure refers to who reports to whom in the company.

d. Intervention.

Incorrect. Organizational intervention refers to management's degree of involvement in the day-to-day operation.

20. If top managers select a goal of rapid company growth, which of the following will have to be changed **first** to meet that growth?

a. Competitive actions

Incorrect. Competitive actions are external actions to a company.

b. Internal actions

Correct. Internal forces for change arise from internal activities and decisions. If top managers select a goal of rapid company growth, internal actions will have to be changed first to meet that growth.

c. External actions

Incorrect. External actions include competitive and regulatory actions.

d. Environmental actions

Incorrect. Environmental actions are external actions.

21. Which of the following is the most common, least intense, and least risky type of change in an organization?

a. Tuning

Correct. Tuning is the most common, least intense, and least risky type of change. Tuning is anticipatory and incremental change.

b. Reorientation

Incorrect. Reorientation change is anticipatory and strategic in scope.

c. Re-creation

Incorrect. Re-creation is most intense and most risky change. Re-creation is reactive and strategic change. It is also called *frame breaking* because it puts organizations to competitive pressures.

d. Adaptation

Incorrect. Adaptation changes are reactive in nature to external pressures, events, or problems. Both tuning and adaptation involve incremental change or continuous improvement (kaizen).

22. Which of the following strategies for overcoming resistance to change should be used when the concern is prevention?

a. Education and communication

Correct. According to Kreitner (*Management*, 9th ed. [Boston: Houghton Mifflin, 2004]), there are six strategies for overcoming resistance to change, including education and communication, participation and involvement, facilitation and support, negotiation and agreement, manipulation and co-optation, and explicit and implicit coercion. The education and communication strategy is appropriate because it teaches prevention rather than cure.

b. Participation and involvement

Incorrect. Participation and involvement increase the stake in success and do not prevent the resistance to change.

c. Facilitation and support

Incorrect. Facilitation and support help to reduce fear and anxiety and do not prevent the resistance to change.

d. Negotiation and agreement

Incorrect. Negotiation and agreement neutralize potential or actual resistance and do not prevent the resistance to change.

23. In project management, each activity has two pairs of durations called:

a. Normal and crash time.

Correct. In project management, each activity has two pairs of duration: normal time and crash time. Normal time is the estimated length of time required to perform an activity, according to the plan. Crash time is the shortest estimated length of time in which the activity can be completed. The other three choices are not relevant here.

b. Normal and budget time.

Incorrect. See correct answer (a).

c. Actual and crash time.

Incorrect. See correct answer (a).

d. Quantity and quality time.

Incorrect. See correct answer (a).

24. In project management, which of the following measures the cost efficiency with which the project is being performed?

a. Cost variance

Incorrect. The cost variance is the difference between the cumulative earned value of the work performed and the cumulative actual cost.

b. Schedule variance

Incorrect. The schedule variance is the difference between cumulative earned value and cumulative planned value.

c. Schedule performance index

Incorrect. The schedule performance index (SPI) is cumulative earned value divided by cumulative planned value.

d. Cost performance index

Correct. The cost performance index (CPI) is a measure of the cost efficiency with which a project is being performed. The formula for calculating the CPI is cumulative earned value divided by cumulative actual cost.

25. In project management, the schedule performance index (SPI) analysis should include identifying those work packages within the project that should be given top priority to work on it **first** is:

a. A negative SPI of 1.0.

Incorrect. See correct answer (c).

b. A positive SPI of 1.0.

Incorrect. See correct answer (c).

c. A negative SPI of 2.0.

Correct. A negative SPI means that the time a work is performed is not in keeping with the actual schedule. It also means that there is a gap between the earned value of the work performed and the planned value. A SPI of less than 1.0 means that for every planned hour actually expended, less than one hour of earned value was received. When the SPI goes below 1.0 or gradually gets smaller, corrective action should be taken. Here, the largest negative value of 2.0 should be given top priority to work on it first.

In terms of negative values, the same logic equally applies to both SPI and cost performance index (CPI). A negative cost variance means that the work performed is not in keeping with the actual cost. It also means that there is a gap between the value of the work performed and the actual costs incurred. A CPI of less than 1.0 means that for every dollar actually expended, less than one dollar of earned value was received. When the CPI goes below 1.0 or gradually gets smaller, corrective action should be taken.

d. A positive SPI of 2.0.

Incorrect. See correct answer (c).

Domain 6: Information Technology and Business Continuity

1. Authorization controls are a part of which of the following?

a. Directive controls.

Incorrect. Directive controls are broad-based controls to handle security incidents, and they include management's policies, procedures, and directives.

b. Preventive controls.

Correct. Authorization controls, such as access control matrices and capability tests, are a part of preventive controls because they block unauthorized access. Preventive controls deter security incidents from happening in the first place.

c. Detective controls.

Incorrect. Detective controls enhance security by monitoring the effectiveness of preventive controls and by detecting security incidents where preventive controls were circumvented.

d. Corrective controls.

Incorrect. Corrective controls are procedures to react to security incidents and to take remedial actions on a timely basis. Corrective controls require proper planning and preparation as they rely more on human judgment.

2. Which of the following is **not** an example of nondiscretionary access control?

a. Identity-based access control

Nondiscretionary access control policies have rules that are not established at the discretion of the user. These controls can be changed only through administrative action, not by users. An identity-based access control decision grants or denies a request based on the presence of an entity on an access control list. Both identity-based access control and discretionary access control are considered equivalent and are not examples of nondiscretionary access controls.

b. Mandatory access control

Incorrect. This is an example of nondiscretionary access controls. Mandatory access control deals with rules.

c. Role-based access control

Incorrect. This is an example of nondiscretionary access controls. Role-based access control deals with job titles and functions.

d. Temporal constraints

Incorrect. This is an example of nondiscretionary access controls. Temporal constraints deal with time-based restrictions and control time-sensitive activities.

3. Which of the following statements are true about access controls, safety, trust, and separation of duty?

I. No leakage of access permissions are allowed to an unauthorized principal.

II. No access privileges can be escalated to an unauthorized principal.

III. No principals' trust means no safety.

IV. No separation of duty means no safety.

a. I only

Incorrect. See correct answer (d).

b. II only. See correct answer (d).

Incorrect.

c. I, II, and III

Incorrect.See correct answer (d).

d. I, II, III, and IV

Correct. If complete trust by a principal is not practical, there is a possibility of a safety violation. The separation of duty concept is used to enforce safety and security in some access control models. In an event where there are many users (subjects), objects, and relations between subjects and objects, safety needs to be carefully considered.

4. For privilege management, which of the following is the correct order?

a. Access control → Access management → Authentication management → Privilege management

Incorrect. See correct answer (c).

b. Access management → Access control → Privilege management → Authentication management

Incorrect. See correct answer (c).

c. Authentication management → Privilege management → Access control → Access management

Correct. Privilege management is defined as a process that creates, manages, and stores the attributes and policies needed to establish criteria that can be used to decide whether an authenticated entity's request for access to some resource should be granted. Authentication management deals with identities, credentials, and any other authentication data needed to establish an identity. Access management, which includes privilege management and access control, encompasses the science and technology of creating, assigning, storing, and accessing attributes and policies. These attributes and policies are used to decide whether an entity's request for access should be allowed or denied. In other words, a typical access decision starts with authentication management and ends with access management. Privilege management falls in between.

d. Privilege management → Access management → Access control → Authentication management

Incorrect. See correct answer (c).

5. The encryption technique that requires two keys, a public key that is available to anyone for encrypting messages and a private key that is known only to the recipient for decrypting messages, is

a. Rivest, Shamir, and Adelman (RSA).

Correct. Rivest, Shamir, and Adelman (RSA) requires two keys: The public key for encrypting messages is widely known, but the private key for decrypting messages is kept secret by the recipient.

b. Data encryption standard (DES).

Incorrect. Data Encryption Standard (DES) requires only a single key for each pair of communicants that want to send each other encrypted messages.

c. Modulator-demodulator.

Incorrect. A modulator-demodulator (modem) is used for telecommunications.

d. A cipher lock.

6. The use of message encryption software:

a. Guarantees the secrecy of data.

Incorrect. No encryption approach absolutely guarantees the secrecy of data in transmission although encryption approaches are considered to be less amenable to being broken than others.

b. Requires manual distribution of keys.

Incorrect. Keys may be distributed manually, but they may also be distributed electronically via secure key transporters.

c. Increases system overhead.

Correct. The machine instructions necessary to encrypt and decrypt data constitute system overhead, which means that processing may be slowed down.

d. Reduces the need for periodic password changes.

Incorrect. Using encryption software does not reduce the need for periodic password changes because passwords are the typical means of validating users' access to unencrypted data.

7. The information systems and audit directors agreed on the need to maintain security and integrity of transmissions and the data they represent. The best means of ensuring the confidentiality of satellite transmissions would be:

a. Encryption.

Correct. Encryption is the best means of ensuring the confidentiality of satellite transmissions because even if an unauthorized individual recorded the transmissions, they would not be intelligible.

b. Access control.

Incorrect. Access control applies to gaining entrance to the application systems, not to the format of transmissions.

c. Monitoring software.

Incorrect. Monitoring software is designed to monitor performance (human or machine) for specified functions such as number of tasks performed or capacity utilized.

d. Cyclic redundancy checks.

Incorrect. Cyclic redundancy checks are complex computations performed with the data bits and the check bits in data transmissions to ensure the integrity, but not the confidentiality, of the data.

8. For application user authenticator management purposes, use of which of the following is risky and leads to stronger alternatives?

a. A single sign-on mechanism

Incorrect. See correct answer (c).

b. Same user identifier and different user authenticators on all systems

Incorrect. See correct answer (c).

c. Same user identifier and same user authenticator on all systems

Correct. Examples of user identifiers includes internal users, contractors, external users, guests, passwords, tokens, and biometrics. Examples of application user authenticators include passwords, PINs, tokens, biometrics, digital certificates based on public key infrastructure, and key cards. When an individual has accounts on multiple information systems, there is the risk that if one account is compromised and the individual uses the same user identifier and authenticator, other accounts will be compromised as well. Possible alternatives include (1) having the same user identifier but different authenticators on all systems, (2) having different user identifiers and different user authenticators on each system, (3) employing a single sign-on mechanism, or (4) having one-time passwords on all systems.

d. Different user identifiers and different user authenticators on each system

Incorrect. See correct answer (c).

9. Which of the following statements is **true** about intrusion detection systems (IDS) and firewalls?

a. Firewalls are a substitute for an IDS.

Incorrect. See correct answer (c).

b. Firewalls are an alternative to an IDS.

Incorrect. See correct answer (c).

c. Firewalls are a complement to an IDS.

Correct. An IDS should be used as a complement to a firewall, not a substitute for it. Together, they provide a synergistic effect.

d. Firewalls are a replacement for an IDS.

Incorrect. See correct answer (c).

10. Which one of the following is **not** an authentication mechanism?

a. What the user knows

Incorrect. This choice is part of an authentication process.

b. What the user has

Incorrect. This choice is part of an authentication process.

c. What the user can do

Correct. "What the user can do" is defined in access rules or user profiles, which come after a successful authentication. The other three choices are part of an authentication process. The authenticator factor "knows" means a password or PIN, "has" means key or card, and "is" means a biometric identity.

d. What the user is

Incorrect. This choice is part of an authentication process.

11. Which of the following is the correct sequence of steps to be followed in an application software change control process?

I. Test the changes.

II. Plan for changes.

III. Initiate change request.

IV. Release software changes.

a. I, II, III, and IV

Incorrect. See correct answer (c).

b. II, I, III, and IV

Incorrect. See correct answer (c).

c. III, II, I, and IV

Correct. Any application software change must start with a change request from a functional user. An information technology person can plan, test, and release the change after approved by the functional user.

d. IV, III, I, and II

Incorrect. See correct answer (c).

12. Software configuration management (SCM) should primarily address which of the following questions?

a. How does software evolve during system development?

Incorrect. See correct answer (c).

b. How does software evolve during system maintenance?

Incorrect. See correct answer (c).

c. What constitutes a software product at any point in time?

Correct. SCM is a discipline for managing the evolution of computer products, during the initial stages of development and through to maintenance and final product termination. Visibility into the status of the evolving software product is provided through the adoption of SCM on a software project. Software developers, testers, project managers, quality assurance staff, and the customer benefit from SCM information. SCM answers questions such as (1) What constitutes the software product at any point in time? and (2) What changes have been made to the software product? How a software product is planned, developed, or maintained does not matter; these issues refer to the history of a software product's evolution, as described in the other choices.

d. How is a software product planned?

Incorrect. See correct answer (c).

13. Security controls are designed and implemented in which of the following system development life cycle (SDLC) phases?

a. Planning/initiation

Incorrect. See correct answer (b).

b. Development/acquisition

Correct. Security controls are developed, designed, and implemented in the development/ acquisition phase. Additional controls may be developed to support the controls already in place or planned. Security controls are not designed and implemented in the other three choices because they are either too early or too late in the life cycle.

c. Implementation/assessment

Incorrect. See correct answer (b).

d. Disposal/decommissioning

Incorrect. See correct answer (b).

14. Which of the following tests is driven by system requirements?

a. Black box testing

Correct. Black box testing, also known as functional testing, executes part or all the system to validate that the user requirement is satisfied.

b. White box testing

Incorrect. White box testing, also known as structural testing or glass box testing, examines the logic of the units and may be used to support software requirements for test coverage (i.e., how much of the program has been executed).

c. Gray box testing

Incorrect. Gray box testing can be looked at as anything that is not tested in white box or black box.

d. Glass box testing

Incorrect. Glass box testing is another name for white box testing.

15. Which of the following volatile data generated by operating system software installed on workstations and servers should be collected first prior to conducting computer forensic auditing work?

I. Network connections

II. Login sessions

III. Network configuration

IV. Operating system time

a. I and II

Correct. Operating system data exists in both nonvolatile and volatile data. "Nonvolatile data" refers to data that persists even after a personal computer is powered down, such as a file system stored on a hard drive or a flash drive. "Volatile data" refers to data on a live system that is lost after a personal computer is powered down, usually stored on random access memory (RAM) of a system.

Because volatile data has a propensity to change over time, the order and timeliness with which volatile data is collected is important. In most cases, system auditors and security analysts should first collect information on network connections and login sessions, because network connections may time out or be disconnected, and the list of users connected to a system at any single time may vary. Volatile data that are less likely to change, such as network configuration and operating system time (choice d), should be collected later, if needed.

b. I and III

Incorrect. See correct answer (a).

c. II and III

Incorrect. See correct answer (a).

d. III and IV

Incorrect. See correct answer (a).

16. Which of the following are the potential advantages of using cloud computing technology to user organizations?

I. They can access data and documents from anywhere and at any time.

II. They can reduce the cost of purchasing additional hardware and software.

III. They can reduce the cost of purchasing additional storage memory devices.

IV. They can implement pay-as-you-go method.

a. I and II

Incorrect. See correct answer (d).

b. I and IV

Incorrect. See correct answer (d).

c. I and III

Incorrect. See correct answer (d).

d. I, II, III, and IV

Correct. Cloud computing technology makes it possible to access a user's information from anywhere at any time stored by a cloud vendor. Now even small organizations can store their information in the cloud, obviating the need to purchase additional hardware and software and additional storage memory devices. User organizations need to buy only the amount of storage space that will be really needed and used, which is referred to as pay-as-you-go method. The best feature of this method is that it allows user organizations to scale their needs either up or down based on the storage space required, and they pay accordingly to a cloud vendor.

17. Which of the following statements is **not** true? A data warehouse is:

a. Distributed.

Correct. Databases can be distributed, but not the data warehouse. A distributed data warehouse can have all the security problems faced by a distributed database. From a security viewpoint, data warehousing provides the ability to centrally manage access to an organization's data regardless of a specific location. A data warehouse is subject oriented, time variant, and static in nature.

b. Subject oriented.

Incorrect. See correct answer (a).

c. Time variant.

Incorrect. See correct answer (a).

d. Static in nature.

Incorrect. See correct answer (a).

18. Which of the following provides an effective security control over the Internet access points or hot spots during remote access and telework?

a. Virtual private network

Correct. A virtual private network (VPN) should be used to encrypt data for hot spot users. A VPN is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. VPNs are intended to provide secure connections between remote clients, such as branch offices or traveling employees and a central office. The networks listed in the other three choices do not have the same security features as the VPN and do not have the same geographic reach as the VPN. The other three networks have limitations in terms of access reach.

b. Wireless personal area network

Incorrect. A wireless personal area network is used to establish small-scale wireless networks such as those using Bluetooth, which is an open standard for short-range communication.

c. Wireless local area network

Incorrect. A wireless local area network is a group of wireless networking nodes within a limited geographic area that serve as an extension to existing wired local area network.

d. Virtual local area network

Incorrect. A virtual local area network (VLAN) is a network configuration in which frames are broadcast within the VLAN and routed between VLANs. VLANs separate the logical topology of the LANs from their physical topology.

19. What does an effective backup method for handling large volumes of data in a local area network (LAN) environment include?

a. Backing up at the workstation.

Incorrect. Backing up at the workstation lacks storage capacity.

b. Backing up at the file server.

Correct. Backing up at the file server is effective for a LAN due to its greater storage capacity.

c. Using faster network connection.

Incorrect. Using faster network connection increases the speed but not backup.

d. Using Redundant Array of Independent Disks Technology.

Incorrect. Redundant Array of Independent Disks (RAID) technology is mostly used for the mainframe.

20. All of the following are examples of security risks over servers **except**:

a. Client/server architecture.

Correct. Client/server architecture makes it possible for a wide range of front-end client applications, such as databases, spreadsheets, and word processors, to simultaneously share the same data. A database server supports a high-performance, multi-user, relational database management system (RDMS). Client/server architecture provides a high level of data integrity, concurrency control, and improved performance.

b. Data concentration.

Incorrect. This is an example of security risks over servers.

c. Attack targets.

Incorrect. This is an example of security risks over servers.

d. A single point of failure.

Incorrect. This is an example of security risks over servers.

21. Which of the following server types is used for protection from malicious code attacks at the network gateway?

a. A web server

Incorrect. See correct answer (d).

b. An image server

Incorrect. See correct answer (d).

c. A mail server

Incorrect. See correct answer (d).

d. A quarantine server

Correct. A quarantine server is used for protection from malicious code attacks at the network gateway. A common technique applied in protecting networks is to use a firewall. In this technique, if a user attempts to retrieve an infected program via File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), or Simple Mail Transfer Protocol (SMTP), it is stopped at the quarantine server before it reaches the individual workstations.

22. Which of the following information technology contingency solutions for servers minimizes the recovery time window?

a. Electronic vaulting

Incorrect. Electronic vaulting provides additional data backup capabilities, with backups made to remote tape or disk drives over communication links.

b. Remote journaling

Incorrect. Remote journaling provides additional data backup capabilities, with backups made to remote tape or disk drives over communication links.

c. Load balancing

Incorrect. Load balancing increases server and application system availability.

d. Disk replication

Correct. With disk replication, recovery windows are minimized because data are written to two different disks to ensure that two valid copies of the data are always available. The two disks are called the protected server (the main server) and the replicating server (the backup server). Electronic vaulting and remote journaling are similar technologies that provide additional data backup capabilities, with backups made to remote tape or disk drives over communication links.

23. Contingency plans for information technology operations should include appropriate backup agreements. Which of the following arrangements would be considered too vendor dependent when vital operations require almost immediate availability of computer resources?

a. A hot site arrangement

Incorrect. A hot site has all needed assets in place and is not vendor dependent.

b. A cold site arrangement

Correct. A cold site has all necessary assets in place except the needed computer equipment and is vendor dependent for timely delivery of equipment.

c. A cold and hot site combination arrangement.

Incorrect. A listed combination allows the hot site to be used until the cold site is prepared and is thus not too vendor dependent.

d. Using excess capacity at another data center within the organization

Incorrect. Excess capacity would ensure that needed assets are available and would not be vendor dependent.

24. From an operations viewpoint, the **first step** in contingency planning is to perform a(n):

a. Operating system software backup.

Incorrect. See correct answer (d).

b. Applications software backup.

Incorrect. See correct answer (d).

c. Documentation backup.

Incorrect. See correct answer (d).

d. Hardware backup.

Correct. Hardware backup is the first step in contingency planning. All computer installations must include formal arrangements for alternative processing capability in the event their data center or any portion of the work environment becomes disabled. These plans can take several forms and involve the use of another data center. Hardware manufacturers and software vendors can be helpful in locating an alternative processing site and in some cases provide backup equipment under emergency conditions. The more common plans are service bureaus, reciprocal arrangements, and hot sites. After hardware is backed up, operating system software is backed up next, followed by applications software backup and documentation.

25. The primary contingency strategy for application systems and data is regular backup and secure offsite storage. From an operations viewpoint, which of the following decisions is **least** important to address?

a. How often the backup is performed

Incorrect. See correct answer (c).

b. How often the backup is stored offsite

Incorrect. See correct answer (c).

c. How often the backup is used

Correct. Normally, the primary contingency strategy for applications and data is regular backup and secure offsite storage. Important decisions to be addressed include how often the backup is performed, how often it is stored offsite, and how it is transported to storage, to an alternative processing site, or to support the resumption of normal operations. How often the backup is used is not relevant because it is hoped that it may never have to be used

d. How often the backup is transported

Incorrect. See correct answer (c).

Domain 7: Financial Management

1. A company uses straight-line depreciation for financial reporting purposes, but uses accelerated depreciation for tax purposes. Which of the following account balances would be **lower** in the financial statements used for tax purposes than it would be in the general purpose financial statements?

a. Accumulated depreciation

Incorrect. The balance of accumulated depreciation would be higher in the financial statements for tax purposes, since higher depreciation expense would be reported under accelerated depreciation than under straight-line depreciation.

b. Cash

Incorrect. Depreciation expense is a noncash charge. The cash balance is unaffected by the depreciation method used.

c. Retained earnings

Correct. Under accelerated depreciation, depreciation expense is higher and net income is lower. Retained earnings would therefore be lower for tax-reporting purposes than for general-purpose financial reporting based on straight-line depreciation.

d. Gross fixed assets

Incorrect. The historic cost of fixed assets is recorded in the gross fixed assets account. The historic cost of the assets is unaffected by the depreciation method used.

2. Under a defined contribution pension plan, (List A) is reported on the balance sheet only if the amount the organization has contributed to the pension trust is (List B) the amount required.

List A List B

a. An asset Greater than

Correct. Under a defined contribution plan, the company reports an asset on the balance sheet only if the contribution to the pension trust is greater than the defined, required contribution.

b. An asset Equal to

Incorrect. An asset is reported only if the contribution is in excess of the required contribution. If the actual contribution is equal to that required, no asset is reported.

c. A liability Greater than

Incorrect. The company would report a liability on the balance sheet only if the contribution was less than the required amount, not greater than the required amount.

d. A liability Equal to

Incorrect. The company would not report a liability on the balance sheet if it contributed the required amount to the pension trust.

3. When a business is acquired, the purchasing company calculates goodwill associated with the acquisition as the difference between the purchase price and the:

a. Book value of the identifiable net assets acquired.

Incorrect. Goodwill is calculated as the difference between the purchase price and the fair market value, not the book value, of identifiable net assets acquired.

b. Fair market value of the identifiable net assets acquired.

Correct. Goodwill is the difference between the purchase price and the fair market value of identifiable net assets acquired.

c. Book value of the net tangible assets acquired.

Incorrect. It is the fair market value of identifiable net assets that is used in calculating goodwill. Further, both tangible and intangible assets are included.

d. Fair market value of the net tangible assets acquired.

Incorrect. The values of both tangible and intangible acquired net assets are included in the goodwill calculation.

4. What conclusion should a financial analyst draw if a company has a high fixed assets turnover ratio?

a. The company may be overcapitalized.

Incorrect. The ratio may indicate just the opposite.

b. The company may have a problem with employees converting inventory to personal use.

Incorrect. The fixed assets turnover ratio is sales divided by net fixed assets; fluctuations in inventory do not affect the ratio.

c. The company may be undercapitalized.

Correct. This high ratio could be an indicator that the company cannot afford to buy enough assets.

d. The company has favorable profitability.

Incorrect. The fixed assets turnover ratio is not a profitability indicator. It is sales divided by net fixed assets.

5. A company will finance next year's capital projects through debt rather than additional equity. The benchmark cost of capital for these projects should be:

a. The before-tax cost of new debt financing.

Incorrect. The cost of capital is a composite, or weighted average, of all financing sources in their usual proportions. The cost of capital should also be calculated on an after-tax basis.

b. The after-tax cost of new debt financing.

Incorrect. The cost of capital is a composite, or weighted average, of all financing sources in their usual proportions. It includes both the after-tax cost of debt and the cost of equity financing.

c. The cost of equity financing.

Incorrect. The cost of capital is a composite, or weighted average, of all financing sources in their usual proportions. It includes both the after-tax cost of debt and the cost of equity financing.

d. The weighted-average cost of capital.

Correct. A weighted-average of the costs of all financing sources should be used, with the weights determined by the usual financing proportions. The terms of any financing raised at the time of initiating a particular project does not represent the cost of capital for the firm.

6. In the distribution of liquidation proceeds for a bankrupt firm, which of the following claimants has **highest** priority?

a. Preferred stock

Incorrect. Preferred shareholders are not among the high priority claimants of a bankrupt firm, ranking ahead of only the common shareholders.

b. Common stock

Incorrect. Common shareholders are the residual claimants of a bankrupt firm. They receive a portion of the liquidation proceeds only after all other claims have been satisfied in full.

c. Bonds payable

Incorrect. Bonds payable are general, unsecured claims. They share in liquidation proceeds only after all priority claimants are satisfied.

d. Taxes payable

Correct. Taxes payable is a priority claim. Priority claims are paid in full before any liquidation proceeds are distributed to general claimants or shareholders.

7. A company has a foreign-currency-denominated trade payable due in 60 days. In order to eliminate the foreign exchange risk associated with the payable, the company could:

a. Sell foreign currency forward today.

Incorrect. The company needs to arrange to buy the foreign currency in order to make payment to the supplier. This cannot be accomplished by a forward market sale of foreign currency.

b. Wait 60 days and pay the invoice by purchasing foreign currency in the spot market at that time.

Incorrect. Waiting to convert the currency in 60 days' time does not eliminate the risk of exchange rate movements.

c. Buy foreign currency forward today.

Correct. The company can arrange today for the exchange rate at which it will purchase the foreign currency in 60 days' time by buying the currency in the forward market. This will eliminate the exchange risk associated with the trade payable.

d. Borrow foreign currency today, convert it to domestic currency on the spot market, and invest the funds in a domestic bank deposit until the invoice payment date.

Incorrect. This strategy would be comparable to a future sale of the foreign currency at a rate known today, which would not provide the currency needed to pay the invoice. The opposite strategy would be an effective money market hedge however. If the company converted domestic currency to foreign currency in the spot market today and invested in a foreign bank deposit or Treasury bill, it could then use the proceeds from the foreign investment to pay the invoice in 60 days' time.

8. The following information pertains to a checking account of a company at July 31, 20XX:

Balance per bank statement	$40,000
Interest earned for July	100
Outstanding checks	3,000
Customers' checks returned or insufficient funds	1,000
Deposit in transit	5,000

At July 31, 20XX, the company's correct cash balance is:

a. $41,100.

Incorrect. The customer's check returned for insufficient funds is erroneously subtracted from the balance per bank statement at July 31, 20XX. The interest earned for July is mistakenly added to the balance per bank statement at July 31, 20XX.

Cash balance per bank statement, July 31, 20XX	$40,000
Deposit in transit, July 31, 20XX	5,000
Outstanding checks, July 31, 20XX	(3,000)
Return of customer's check for insufficient funds	(1,000)
Interest earned for July 20XX	100
Incorrect cash balance, July 31, 20XX	$41,100

b. $41,000.

Incorrect. The amount of the customer's check returned for insufficient funds is erroneously subtracted from the balance per bank statement at July 31, 20XX.

Cash balance per bank statement, July 31, 20XX	$40,000
Deposit in transit, July 31, 20XX	5,000
Outstanding checks, July 31, 20XX	(3,000)
Return of customer's check for insufficient funds	(1,000)
Incorrect cash balance, July 31, 20XX	$41,000

c. $42,100.

Incorrect. The interest earned for July is erroneously added to the balance per bank statement at July 31, 20XX.

Cash balance per bank statement, July 31, 20XX	$40,000
Deposit in transit, July 31, 20XX	5,000
Outstanding checks, July 31, 20XX	(3,000)
Interest earned for July 20XX	100
Incorrect cash balance, July 31, 20XX	$42,100

d. $42,000.

Correct. The company's correct cash balance of $42,000 at July 31, 20XX, is computed as:

Cash balance per bank statement, July 31, 20XX	**$40,000**
Deposit in transit, July 31, 20XX	**5,000**
Outstanding checks, July 31, 20XX	**(3,000)**
Correct cash balance, July 31, 20XX	**$42,000**

The bank statement already reflects the interest earned and NSF check.

9. An organization borrows funds from its bank for a one-year period. The bank charges interest at a nominal rate of 15% per annum, on a discount basis, and requires a 10% compensating balance. The effective annual interest rate on the loan is:

a. 16.67%.

Incorrect. This solution does not adjust for the discount interest arrangement on the loan but does adjust the nominal rate for the compensating balance requirement as:

$$\text{Effective annual interest rate} = \frac{\text{Nominal rate (fraction)}}{1 - \text{Compensating balance (fraction)}}$$

$$= .15/(1 - .1) = .1667, \text{ or } 16.67\%$$

b. 17.65%.

Incorrect. This solution adjusts for the discount interest arrangement, but does not adjust the nominal rate for the compensating balance requirement, as:

$$\text{Effective annual interest rate} = \frac{\text{Nominal rate (fraction)}}{1 - \text{Nominal rate (fraction)}}$$

$$= .15/(1 - .15) = .1765, \text{ or } 17.65\%$$

c. 20.00%.

Correct. The effective annual interest rate on the loan is 20.00%. It is increased by both the discount interest arrangement and by the compensating balance requirement. It is calculated as:

$$\textbf{Effective rate} = \frac{\textbf{Nominal rate (fraction)}}{\textbf{1 – Nominal rate (fraction) – Compensating balance (fraction)}}$$

$$\textbf{= .15/(1 – .15 – .1) = .20, or 20.00\%}$$

d. 25.00%.

Incorrect. This is the sum of the nominal rate of 15% and the 10% compensating balance requirement, not the effective annual interest rate.

10. The cost of materials has risen steadily over the year. The company uses its newest materials first when removing items from inventory. Which of the following methods of estimating the ending balance of the materials inventory account will result in the **highest** net income, all other variables held constant?

a. Last in, first out (LIFO).

Incorrect. The last in, first out (LIFO) method assumes that the most recent and hence costliest units have been removed from inventory. This method will result in the lowest inventory balance if costs rise steadily during the accounting period, the highest cost of goods sold, and the lowest net income.

b. First in, first out (FIFO).

Correct. The first in, first out (FIFO) method assumes that the oldest and hence least costly units have been removed from inventory. This method will result in the highest inventory balance if costs rise steadily during the accounting period. This then results in the lowest cost of goods sold and therefore the highest net income.

c. Weighted average.

Incorrect. The weighted-average cost method will average the cost of all inventory items and will result in a lower inventory balance and net income than does the FIFO method.

d. Specific identification.

Incorrect. Specific identification charges the actual cost of each unit to cost of goods sold each period, leaving as inventory the actual cost of all items still in inventory. Since the question states that the newest and most costly items are removed from inventory first, the inventory balance and net income will be lower than that obtained using FIFO estimation.

11. General sales taxes tend to be regressive with respect to income because:

a. A larger portion of a poor person's income is subject to the tax.

Correct. Rich people avoid the general sales tax on the portion of their income that is saved whereas poor people are unable to save.

b. A smaller portion of a poor person's income is subject to the tax.

Incorrect. The opposite is true.

c. The tax rate is higher for the poor.

Incorrect. The tax rate is uniform for all taxpayers in a general sales tax.

d. The tax claims an increasing amount of income as income rises.

Incorrect. General sales tax does not claim an increasing amount of income as income rises. This statement is a description of a progressive, not a regressive, tax.

12. During the current accounting period, a manufacturing company purchased $70,000 of raw materials, of which $50,000 of direct materials and $5,000 of indirect materials was used in production. The company also incurred $45,000 of total labor costs and $20,000 of other factory overhead costs. An analysis of the work-in-process control account revealed $40,000 of direct labor costs. Based on the above information, what is the total amount accumulated in the factory overhead control account?

a. $25,000

Incorrect. The $25,000 amount includes only two of the three factory overhead costs.

b. $30,000

Correct. The total amount accumulated in the factory overhead control account is $30,000 and is computed as shown.

The factory overhead control account should have these costs:

Indirect materials	**$5,000**
Indirect labor ($45,000 – $40,000)	**5,000**
Other factory overhead	**20,000**
Total overhead	**$30,000**

c. $45,000

Incorrect. The $45,000 amount includes additional costs, which are not classified as factory overhead costs.

d. $50,000

Incorrect. The $50,000 amount also includes additional costs, which are not classified as factory overhead costs.

13. A company experienced a machinery breakdown on one of its production lines. As a consequence of the breakdown, manufacturing fell behind schedule, and a decision was made to schedule overtime in order to return manufacturing to schedule. Which one of the following methods is the proper way to account for the overtime paid to the direct laborers?

a. The overtime hours times the sum of the straight-time wages and overtime premium would be charged entirely to manufacturing overhead.

Incorrect. This treatment is inappropriate because only the overtime premium times the overtime hours is charged to overhead. The straight-time wages times the overtime hours should still be treated as direct labor.

b. The overtime hours times the sum of the straight-time wages and overtime premium would be treated as direct labor.

Incorrect. This treatment is inappropriate because only the straight-time wages times the overtime hours should still be treated as direct labor. The overtime premium times the overtime hours is charged to overhead.

c. The overtime hours times the overtime premium would be charged to repair and maintenance expense while the overtime hours times the straight-time wages would be treated as direct labor.

Incorrect. While the second part of this response is correct, the first part is inappropriate. There is no way that the overtime hours times the premium can be charged to repair and maintenance expense because this cost is not related to any repairs. This work is production work, not repairs.

d. The overtime hours times the overtime premium would be charged to manufacturing overhead while the overtime hours times the straight-time wages would be treated as direct labor.

Correct. This treatment is appropriate because the overtime premium cost is a cost that should be borne by all production.

14. A company has analyzed seven new projects, each of which has its own internal rate of return (IRR). It should consider each project whose internal rate of return is _____ its marginal cost of capital (MCC) and accept those projects in _____ order of their IRR.

a. Below; decreasing.

Incorrect. The company only accepts projects whose IRR exceeds the MCC.

b. Above; decreasing.

Correct. When a project's IRR is greater than its marginal cost, it increases the value of the firm's stock since a surplus remains after paying for the capital.

c. Above; increasing.

Incorrect. It should rank IRRs from highest to lowest.

d. Below; increasing.

Incorrect. It should rank IRRs from highest to lowest and should only accept projects whose IRR exceeds the MCC.

15. An existing machine with estimated remaining life of five years that cost $100,000 can be sold for $20,000. The variable cost of output from this machine has been $1 per unit with 100,000 units per year produced. A new machine will cost $90,000 and is estimated to lower the variable cost to $.70 per unit over its five-year life. The most appropriate term for the decision process involved in this scenario is:

a. Capital budgeting.

Correct. Capital budgeting is the term for deciding on long-term investments such as the one described.

b. Economic order quantity.

Incorrect. This deals with the quantity of goods to order at a time, which will minimize the total of order and storage costs during the period.

c. Flexible budgeting.

Incorrect. This deals with short- term adjustments of a budget to conform to actual production or sales.

d. Sensitivity analysis.

Incorrect. This deals with any instance in which a range of outcome is possible and is not restricted to long-term investment decisions.

16. Many service industries utilize a budgeting process to identify major programs and develop short-term operating budgets, such as expected revenues and expected direct expenses, for the identified programs. For example, a nursing home may develop one-year revenue and expense budgets for each of its different programs, such as day care for the elderly or Meals on Wheels. Which of the following is a **major** advantage of short-term program planning and budgeting?

a. It eliminates the need for periodic program evaluation.

Incorrect. Short-term program planning and budgeting provides the basis for periodic program evaluation.

b. It provides a rigid basis for periodic program evaluation.

Incorrect. The administration of budgets should never be rigid, as changed conditions call for changes in the budget.

c. It promotes communication and coordination within an organization.

Correct. Promotion of communication and coordination is a major advantage of short-term program planning and budgeting.

d. It provides an important basis for strategic analysis of the goals of the organization.

Incorrect. Strategic analysis is long-term rather than short-term in nature, and usually precedes the development of short-term budgets.

17. Actual and projected sales of a company for September and October are:

	Cash sales	Credit sales
September (actual)	$20,000	$50,000
October (projected)	30,000	55,000

All credit sales are collected in the month following the month in which the sale is made. The September 30 cash balance is $23,000. Cash disbursements in October are projected to be $94,000. To maintain a minimum cash balance of $15,000 on October 31, the company will need to borrow:

a. $0.

Incorrect. See correct answer (b).

b. $ 6,000.

Correct. The company will need to borrow $6,000, computed as:

Ending cash balance
= Beginning cash balance + Cash collections
– Cash disbursements
= $23,000 + (50,000 + 30,000) – 94,000 = $ 9,000

Borrowing = $15,000 – 9,000 = $6,000

Therefore, by definition, the other choices will be incorrect.

c. $11,000.

Incorrect. See correct answer (b).

d. $16,000.

Incorrect. See correct answer (b).

18. Which of the following is **not** true about international transfer prices for a multinational firm?

a. They allow firms to attempt to minimize worldwide taxes.

Incorrect. Properly chosen transfer prices allow firms to attempt to minimize worldwide taxes by producing various parts of the products in different countries and strategically transferring the parts at various systematically calculated prices.

b. They allow the firm to evaluate each division.

Incorrect. Properly chosen transfer prices allocate revenues and expenses to divisions in various countries. These numbers are used as part of the input for the performance evaluation of each division.

c. They provide each division with a profit-making orientation.

Incorrect. Transfer prices motivate division managers to buy parts and products (from either internal or external suppliers) at the lowest possible prices and to sell their products (to either internal or external customers) at the highest possible prices. This provides each division with a profit-making orientation.

d. They allow firms to correctly price products in each country in which they operate.

Correct. The calculation of transfer prices in the international arena must be systematic. A scheme for calculating transfer prices for a firm may correctly price the firm's product in Country A but not in Country B. The product may be overpriced in Country B, and sales will be lower than anticipated. Alternatively, the product may be underpriced in Country B, and authorities there may allege that the firm is dumping its product in Country B.

19. One department of an organization, Final Assembly, is purchasing subcomponents from another department, Materials Fabrication. The price that Materials Fabrication will charge Final Assembly is to be determined. Outside market prices for the subcomponents are available. Which of the following is the **most correct** statement regarding a market-based transfer price?

a. Marginal production cost transfer prices provide incentives to use otherwise idle capacity.

Incorrect. Marginal production cost does not relate to market-based transfer prices.

b. Market transfer prices provide an incentive to use otherwise idle capacity.

Incorrect. Transfer prices based on marginal cost provide more of an incentive to the purchasing division to buy internally and thus use idle facilities of the selling division than the usually higher market-based transfer price.

c. Overall long-term competitiveness is enhanced with a market-based transfer price.

Correct. Market-based transfer prices provide market discipline. Inefficient internal suppliers will tend to wither while efficient ones prosper, enhancing the overall long-term competitiveness of the firm.

d. Corporate politics is more of a factor in a market-based transfer price than with other methods.

Incorrect. Corporate politics is less of a factor in market-based prices than in other methods, such as a negotiated transfer price, because market-based prices are objective.

20. A company makes a product that sells for $30. During the coming year, fixed costs are expected to be $180,000, and variable costs are estimated at $26 per unit. How many units must the company sell in order to break even?

a. 6,000

Incorrect. It ignores variable costs. Total unit sales needed to cover fixed costs only are $180,000/$30.

b. 6,924

Incorrect. This is total fixed costs divided by variable costs per unit.

c. 45,000

Correct. The company must sell 45,000 units to break even. This is computed as:

The contribution to overhead for each unit is $4.00.

Fixed costs of $180,000 divided by the contribution of $4.00 produces the answer of $45,000.

d. 720,000

Incorrect. This is total fixed costs multiplied by the contribution to overhead of $4.00 per unit instead of divided by it.

21. In its first year of operations, a firm had $50,000 of fixed operating costs. It sold 10,000 units at a $10 unit price and incurred variable costs of $4 per unit. If all prices and costs will be the same in the second year and sales are projected to rise to 25,000 units, what will the degree of operating leverage (the extent to which fixed costs are used in the firm's operations) be in the second year?

a. 1.25

Incorrect. This solution incorrectly uses total revenue, rather than contribution to fixed costs, in the degree of operating leverage formula as:

DOL = Q(P) / [Q(P) – F]
= 25,000($10)/ [25,000($10) – $50,000]
= 250,000/200,000 = 1.25

b. 1.50

Correct. The projected degree of operating leverage is 1.50, and calculated as:

DOL = Q(P – V) / [Q(P – V) – F]
= 25,000($10 – $4)/ [25,000($10 – $4) – $50,000]
= 150,000/100,000 = 1.50

where

DOL = degree of operating leverage

Q = Units sold
P = Unit price
V = Unit variable cost
F = Fixed operating costs

c. 2.00

Incorrect. This solution uses the year 1 sales level of 10,000 units and also uses total revenue, rather than the contribution to fixed costs, in calculating the degree of operating leverage as:

DOL = Q(P) / [Q(P) – F]
= 10,000($10)/ [10,000($10) – $50,000]
= 100,000/50,000 = 2.00

d. 6.00

Incorrect. This solution incorrectly uses the year one sales level of 10,000 units in calculating the degree of operating leverage as:

DOL = Q(P – V) / [Q(P – V) – F]
= 10,000($10 – $4)/ [10,000($10 – $4) – $50,000]
= 60,000/10,000 = 6.00

22. A company has 7,000 obsolete toys, which are carried in inventory at a manufacturing cost of $6 per unit. If the toys are reworked for $2 per unit, they could be sold for $3 per unit. If the toys are scrapped, they could be sold for $1.85 per unit. Which alternative is more desirable (rework or scrap), and what is the total dollar amount of the advantage of that alternative?

a. Scrap, $5,950

Correct. The total dollar amount of the advantage of that alternative is scrap, $5,950 and is computed as:

(3 – 2)(7,000) = $ 7,000 for rework

(1.85)(7,000) = $12,950 for scrap

Advantage of scrap by $5,950. That is $12,950 – $7,000 = $5,950.

b. Rework, $36,050

Incorrect. (6 + 3 – 2)(7,000) – (1.85)(7,000) = $36,050 (rework).

c. Scrap, $47,950

Incorrect. (1.85 + 6)(7,000) – (3 – 2)(7,000) = $47,950 (scrap).

d. Rework, $8,050

Incorrect. (3)(7,000) – (1.85)(7,000) = $8,050 (rework).

23. Which of the following statements about activity-based costing (ABC) is **not** true?

a. ABC is useful for allocating marketing and distribution costs.

Incorrect. This is a true statement.

b. ABC is more likely to result in major differences from traditional costing systems if the firm manufactures only one product rather than multiple products.

Correct. When there is only one product, the allocation of costs to the product is trivial. All of the cost is assigned to the one product; the particular method used to allocate the costs does not matter.

c. In ABC, cost drivers are what cause costs to be incurred.

Incorrect. This is a true statement.

d. ABC differs from traditional costing systems in that products are not cross-subsidized.

Incorrect. This is a true statement.

24. The following information is available from the records of a manufacturing company that applies factory overhead based on direct labor hours:

Estimated overhead cost	$500,000
Estimated labor hours	200,000 hours
Actual overhead cost	$515,000
Actual labor hours	210,000 hours

Based on this information, overhead would be:

a. Underapplied by $9,524.

Incorrect. It reflects overhead application based on the estimated volume times an application rate based on the actual overhead over the actual volume. The application rate would be $24,5238, and the applied overhead would be $490,476, which results in underapplied overhead by $9,524 (i.e., $500,000 – $490,476).

b. Overapplied by $10,000.

Correct. Overhead would be overapplied by $10,000 and is computed as:

Applied overhead equals the actual labor hours times the estimated application rate ($2.50 per direct labor hour), or $525,000. This amount is $10,000 higher than the actual overhead cost incurred of $515,000 (i.e., $525,000 – $515,000).

c. Overapplied by $15,000.

Incorrect. This is simply the actual overhead cost less the estimated overhead cost and does not reflect any application, whether over or under (i.e., $515,000 – $500,000).

d. Overapplied by $40,750.

Incorrect. This reflects overhead application based on the actual volume times an application rate based on the actual overhead over the estimated volume. The application rate would be $2.575 per hour and the applied overhead would be $540,750, resulting in overapplied overhead by $40,750 (i.e., $540,750 – $500,000).

25. A company plans to implement a bonus plan based on segment performance. In addition, the company plans to convert to a responsibility accounting system for segment reporting. The following costs, which have been included in the segment performance reports that have been prepared under the current system, are being reviewed to determine if they should be included in the responsibility accounting segment reports.

1. Corporate administrative costs allocated on the basis of net segment sales
2. Personnel costs assigned on the basis of the number of employees in each segment
3. Fixed computer facility costs divided equally among each segment
4. Variable computer operational costs charged to each segment based on actual hours used times a predetermined standard rate; any variable cost efficiency or inefficiency remains in the computer department

Of these four cost items, the only item that could logically be included in the segment performance reports prepared on a responsibility accounting basis would be the:

a. Corporate administrative costs.

Incorrect. The corporate administrative cost item should be excluded from the performance report because the segments have no control over the cost incurrence, or the allocation basis (i.e., the allocation depends on the segment sales [controllable] as well as the sales of other segments [uncontrollable]).

b. Personnel costs.

Incorrect. The personnel cost item should be excluded from the performance report because the segments have no control over the cost incurrence or the method of assignment,(i.e., the assignment depends on the number of employees in the segment [controllable] in proportion to the total number of employees in all segments [not controllable]).

c. Fixed computer facility costs.

Incorrect. The fixed computer facility cost item should be excluded from the performance report because the segments have no control over the cost, and the equal assignment is arbitrary, bearing no relation to usage.

d. Variable computer operational costs.

Correct. Variable computer operational costs. This is the only cost item that can be included in the segment performance report. First, the segments are being charged for actual usage, which is under each segment's control. The predetermined standard rate is set at the beginning of the year which is known by the segment managers, and the efficiencies and inefficiencies of the computer department are not being passed on to the segments; both of these procedural methods promote a degree of control by the segments.

Domain 8: Global Business Environment

1. Which type of organization uses a very high degree of local decision making, evaluation, and control?

   a. Polycentric

   Correct. A polycentric attitude leads to a loose confederation of comparatively independent subsidiaries, rather than to a highly integrated structure. It uses a high degree of local decision making, evaluation, and control.

   b. Geocentric

   Incorrect. A geocentric attitude is necessary in today's competitive global marketplace. Geocentric companies are truly world oriented and favor no specific country. Both local and worldwide objectives are balanced in all aspects of operations.

   c. Ethnocentric

   Incorrect. Ethnocentric companies place emphasis on their home countries. An ethnocentric attitude assumes that the home country's personnel and ways of doing things are best. Authority and decision making are centered in headquarters.

   d. Polychronic

   Incorrect. The term "polychromic" has no meaning here.

2. Which of the following is vital to communication in high-context culture?

   a. Being on time

   Incorrect. See correct answer (b).

   b. Nonverbal and situational cues

   Correct. In high-context culture, people tend to emphasize nonverbal messages when communicating. The other person's official status, place in society, and reputation say a great deal about the person's rights, obligations, and trustworthiness.

   c. Being polite

   Incorrect. See correct answer (b).

   d. Written contacts

   Incorrect. See correct answer (b).

3. To enter foreign markets, most firms begin with which of the following strategies?

   a. Exporting

   Correct. Exporting is the first stage in the internationalization process where goods produced in one country are sold to customers in foreign countries. Exports amount to a large and growing part of the U.S. economy. Exporting enables a country to market its products in other countries using modest resources and with limited risk. With exporting, the corporation maintains its production facilities within the home country and transfers its products for sales in foreign countries.

   b. Licensing

   Incorrect. See correct answer (a).

   c. Direct foreign investment

   Incorrect. See correct answer (a).

   d. Joint ventures

   Incorrect. See correct answer (a).

4. Which of the following **best** describes a transnational company?

   a. Centralized authority and distinct national identity

   Incorrect. This choice does not describe a transnational company.

   b. Decentralized authority and distinct national identity

   Incorrect. This choice does not describe a transnational company.

   c. Decentralized authority and no distinct national identity

   Correct. A transnational company has a decentralized authority structure and no distinct national identity.

   d. Centralized authority and no distinct national identity

   Incorrect. This choice does not describe a transnational company.

5. In addition to the four basic requirements of a contract, which of the following must also occur in order to have a valid contract?

a. The agreement always must be in writing.

Incorrect. See correct answer (c).

b. There must be evidence of undue influence.

Incorrect. See correct answer (c).

c. There must be an absence of an invalidating contract.

Correct. There must be an absence of an invalidating contract, such as duress, undue influence, misrepresentation, or mistake. That is, the purpose should be legal. The four basic requirements include mutual assent, consideration, legality of object, and capacity.

d. A legal remedy need not be available for there to be a breach.

Incorrect. See correct answer (c).

6. Some economic indicators lead the economy into a recovery or recession, and some lag it. An example of a lag variable would be:

a. Chronic unemployment.

Correct. Initial claims of unemployment is a lead indicator, but chronic unemployment is a lag variable.

b. Orders for consumer and producer goods.

Incorrect. Orders for consumer and producer goods lead the economy.

c. Housing starts.

Incorrect. Housing starts lead the economy.

d. Consumer expectations.

Incorrect. Consumer expectations lead the economy.

7. The two main variables that contribute to increases in a nation's real gross domestic product (GDP) are labor productivity and:

a. Definition of the labor force.

Incorrect. The definition of the labor force would not affect the total hours worked.

b. Inflation rate.

Incorrect. The word "real" means discounting for inflation.

c. Quality of output.

Incorrect. National income accounts do not address the quality of output.

d. Total worker hours.

Correct. The major components of real GDP are total worker hours and labor productivity.

8. If a country uses trade quotas to overcome chronic trade deficits, the most likely outcome is:

a. Unemployment and productivity rates will rise.

Incorrect. See correct answer (d).

b. Unemployment rates will rise and productivity rates will decline.

Incorrect. See correct answer (d).

c. Unemployment rates will decline and productivity rates will rise.

Incorrect. See correct answer (d).

d. Unemployment and productivity rates will decline.

Corrrect. With trade quotas, home country jobs will be saved, hence unemployment will decline. Since jobs will be saved for inefficient industries (less efficient than foreign competitors), productivity rates will decline because home countries will not be specializing in those goods with which they have a comparative advantage.

9. Revenue tariffs are designed to:

a. Develop new export opportunities.

Incorrect. Revenue tariffs deal with import, not export, opportunities.

b. Provide the government with tax revenues.

Correct. Revenue tariffs are usually applied to products that are not produced domestically. Their purpose is to provide the government with tax revenues.

c. Restrict the amount of a commodity that can be imported in a given period.

Incorrect. Import quotas are designed to restrict the amount of a commodity, which can be imported in a period of time.

d. Encourage foreign companies to limit the amount of their exports to a particular country.

Incorrect. Voluntary export restrictions, which have the same effect as import quotas, encourage foreign firms to limit their exports to a particular country.

10. Which of the following creates the **most** restrictive barrier to exporting to a country?

a. Tariffs

Incorrect. A tariff is a tax levied by a foreign government against certain imported products. Firms exporting to that country must accept lower profits, absorbing the tariff, or increase selling prices in the foreign country to compensate. This reduces profitability and/or competitiveness in the foreign market but does not exclude the firm from exporting to that country.

b. Quotas

Incorrect. A quota is a limit set by a foreign government on the amount of goods that the importing country will accept in certain product categories. The effect of a quota is to restrict the quantity the firm can export to that country, but not to exclude the firm from selling in that market. The effect on revenues and profitability depends on market conditions in that country.

c. Embargoes

Correct. Embargoes are total bans on some kinds of imports. As such, they are an extreme form of import quotas. Embargoes have the effect of totally excluding the exporting firms from selling in that country and are the most restrictive type of import/export law.

d. Exchange controls

Incorrect. Exchange controls limit the amount of foreign exchange that can be transacted and/or the exchange rate against other currencies. These controls limit the ability of a firm selling in the country to repatriate its export earnings but do not exclude the firm from selling in that market.

Glossary

This glossary contains terms useful key CIA Exam candidates. Reading the glossary terms prior to studying the theoretical subject matter covered in the review books and prior to answering the online test bank's practice questions can help the candidate understand the domain contents better. In addition, this glossary is a good source for answering the multiple-choice questions on the CIA Exam. Risk-related terms are repeated in Part 1, 2, and 3 glossary sections for students' convenience and due to their common topics and the fact that each Part Exam must be passed separately.

40/40/30 rule
This rule identifies the sources of scrap, rework, and waste in manufacturing operations which are approximated to 40% product design, 30% manufacturing processing, and 30% from suppliers.

ABC analysis
ABC analysis is an application of Pareto's law, or the 80/20 rule, to inventory or purchasing. It is a determination of the relative ratios between the number of items and the dollar value of the items purchased repetitively for stock.

Abort
An abort is an abnormal termination of computer program execution prior to its completion.

Acceptance testing
Acceptance testing is one of the phases in the system development life cycle methodology where users and/or independent testers are involved in testing and accepting the system based on the test plan and results. It enables system users to determine whether to accept the system.

Access
Access is a specific type of interaction between a subject (e.g., user) and an object (e.g., data) that results in the flow of information from one to the other.

Access control list
The access control list (ACL) specifies who or what is allowed to access the object and what operations (e.g., modify or delete) are allowed to be performed on the object. It deals with relationships between subjects (e.g., individual users, group of users, processes, and devices) and objects (e.g., programs, files, databases, directories, and devices).

Access time
Access time is the time it takes for the control section of the central processing unit to locate program instruction and data for processing. Another definition for hard disks: Access time is the time that elapses between when the operating system issues an order for data retrieval

and the time the data are ready for transfer from the disk. The access time of a PC disk drive is determined by: seek time (the time the disk heads take to move to the correct track), settle time (the time the heads take to settle down after reaching the correct track), and latency time (the time required for the correct sector to swing around under the head).

Actionable subsidies

Actionable subsidies are those subsidies that are not specifically prohibited under the subsidies agreement, but against which General Agreement on Tariffs and Trade remedies can be sought if they are found to distort trade. Trade distortion occurs if (1) subsidized imports cause injury to a domestic industry (e.g., depress prices or threaten to do so); (2) subsidies nullify or impair benefits owed to another country under the World Trade Organization; or (3) subsidized products displace or impede imports from another country or another country's exports to a third-country market.

Active content

Active content technologies allow code, often in the form of a script, macro, or other mobile code representation, to execute when the document is rendered. Hypertext Markup Language (HTML) and other related markup language documents, whether delivered via Hypertext Transfer Protocol (HTTP) or another means, provide rich mechanisms for conveying executable content. Examples of active content include Postscript and PDF documents; Web pages containing Java applets and JavaScript instructions; and word processor files containing macros, spreadsheet formulas, and other interpretable content. Active content may also be distributed embedded in e-mail or as executable mail attachments. Countermeasures against active content documents include security policy, application settings, automated filters, software version control, software readers, and system isolation.

Activity analysis

Activity analysis is a decision-making tool. All current activities can be labeled as either value added or non–value added using a T-account diagram. The goal is to eliminate or reduce non–value-added activities since they are adding little or no value to the process at hand. Decisions affecting costs incurred for non–value-added activities can then be challenged or revisited by performing a detailed analysis of all tasks and activities with the purpose of eliminating or reducing them. A T-column can be used with headings "Value-added activities" and "Non–value-added activities" to facilitate the activity analysis.

Adaptive maintenance

Adaptive maintenance is any effort initiated as a result of changes in the environment in which a software must operate.

Administered price

An administered price is a price determined by the policy of a seller rather than by the marketplace.

Administrative security

Administrative security is the management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data, programs, equipment, and physical facilities.

Ad valorem

Ad valorem is any charge, tax, or duty that is applied as a percentage of value.

Ad valorem subsidization

Ad valorem subsidization is a percentage amount that is determined by dividing the appropriately allocated and amortized financial value of the subsidy by the sales of the product in question.

Advanced encryption standard

The advanced encryption standard (AES) specifies a cryptographic algorithm that can be used to protect electronic data that is sensitive but unclassified material. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Adware

Adware a software program intended for marketing purposes, such as to deliver and display advertising banners or pop-ups to the user's computer screen or track the user's online usage or purchasing activity. Adware tracks a user's activity and passes it to third parties without the user's knowledge or consent. Click fraud is possible with adware because it involves deceptions and scam that inflate advertising bills with improper charges per click in an online advertisement on the Web. This software application displays advertising in pop-up windows or a bar in the frame of the application window when the program is running.

Afterimage

An afterimage is the image of a database record after it has been updated by an application program.

Alliances

Firms with unique strengths join alliances to be more effective and efficient than their competitors. *See* Partnership/alliance.

Allocation

Allocation is the process of assigning a computer resource, such as disk and tape/cartridge storage, to a specific task.

Alternative risk transfer tools

There are five alternative risk-transfer tools.

Captive insurance methods. A noninsurance firm is created for the purpose of accepting the risk of the parent firm who owns an insurer. Here, a parent firm establishes a subsidiary (called captive insurance company) to finance its retained losses. Captives combine risk transfer and risk retention.

Financial insurance contracts. These contracts are based on spreading risk over time, as opposed to across a pool of similar exposures. These contracts usually involve a sharing of the investment returns between the insurer and the insured.

Multiline/multiyear insurance contracts. These contracts combine a broad array of risks (multiline) into a contract with a policy period that extends over multiple years (multiyear). For example, a pure risk may be combined with a financial risk.

Multiple-trigger policies. These policies reflect the source of the risk and are not as important as the impact of the risk on the earnings of the firm. A pure risk is combined with a financial risk. The policy is "triggered," and payment is made, only upon the occurrence of an adverse event.

Risk securitization. This method involves the creation of securities, such as bonds, or derivatives contracts, options, swaps, or futures, that have a payout or price movement linked to an insurance risk. Examples include catastrophe options, earthquake bonds, catastrophe bonds, and catastrophe equity puts.

Multiple-trigger policies and risk securitization tools are more commonly used risk transfer methods.

Anticipation inventory

An anticipation inventory is an inventory accumulated for a well-defined future need.

Anticircumvention laws
Anticircumvention laws seek to eliminate the ability of exporters to evade or avoid antidumping duties by changing the sites of a product's assembly. Circumvention of antidumping orders has resulted in respondents having to bring repeated dumping cases against the same defendants after they have moved their assembly operations to a new site.

Antidumping laws
Antidumping laws involve a system of regulations to remedy dumping.

Antidumping measures
Antidumping measures involve a duty or fee imposed to neutralize the injurious effect of unfair pricing practices.

Antitrust laws
Antitrust laws are laws that prohibit monopolies, restraint of trade, and conspiracies to inhibit competition. The apply to unfair methods of competition that have a direct, substantial, and reasonably foreseeable effect on the domestic, import, or export commerce of the United States.

Applets
Applets are small applications written in various programming languages that are automatically downloaded and executed by applet-enabled World Wide Web browsers. Examples include Active X and Java applets, both of which have security concerns.

Application program/system
An application program or system is intended to serve a business or nonbusiness function and has a specific input, processing, and output activities (e.g., accounts receivable and general ledger system).

Application program interface (API)
APIs include calls, subroutines, or software interrupts that comprise a documented interface so that a higher-level program, such as an application program, can make use of the lower-level services and functions of another application, operating system, network operating system, or a driver. APIs can be used to write a file in an application program's proprietary format, communicate over a TCP/IP network, access a SQL database, or surf the Internet, which can be risky because APIs can cause buffer overflow exploits that, in turn, lead to worm attacks.

Applied tariff rate
An applied tariff rate is a rate that a General Agreement on Tariffs and Trade (GATT) member country actually applies to imports from its trading partners. GATT is later changed to World Trade Organization (WTO).

Appraisal costs
Appraisal costs are costs associated with measuring, evaluating, or auditing products to ensure conformance with quality standards and performance requirements. Some major cost categories included in this cost classification are purchasing appraisal costs, qualifications of supplier product, equipment calibration, receiving and shipping inspection costs, tests, and product quality audits. These costs are associated with poor quality of products or services.

Arbitrage
Arbitrage is an equalization of foreign exchange rates involving more than two countries.

Archiving
Archiving is the practice of moving seldom-used data or programs from the active database to secondary storage media, such as magnetic tape or cartridge.

As-is process model
An as-is process model is model that portrays how a business process is currently structured. In process improvement efforts, it is used to establish a baseline for measuring subsequent business improvement actions and progress.

Assignable cause
An assignable cause is a source of variation in a process that can be isolated from random causes of variation. It is synonymous with special cause.

Asynchronous communication
Asynchronous communication is a method of data communication in which the transmission of bits of data is not synchronized by a clock signal but is accomplished by sending the bits one after another, with a start bit and a stop bit to mark the beginning and end of the data unit. The two communicating devices must be set to the same speed (the baud rate). Parity also may be used to check each byte transferred for accuracy. Asynchronous communication is popular among personal computers. Because of the lower communication speeds, normal telephone lines can be used for asynchronous communication.

Attribute listing
An attribute listing emphasizes the detailed observation of each particular characteristic or quality of an item or situation. Attempts are then made to profitably change the characteristic or to relate it to a different item.

Auditability
The term "auditability" refers to features and characteristics that allow verification of the adequacy of procedures and controls and of the accuracy of processing transactions and results in either a manual or an automated system.

Authenticate
To authenticate is to establish the validity of a claimed identity.

Authentication
Authentication is the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

Authoritative Decision Making
The term "authoritative decision making" refers to a style of decision making in which the leader makes a decision and instructs followers what to do without consulting or involving them in the decision-making process.

Authority
Authority is the formal and legitimate right of a manager to make decisions, issue orders, and allocate resources to achieve organizationally desired outcomes.

Authorization
Authorization implies that the authorizing authority has verified and validated that the activity or transaction conforms to established policies and procedures. It is a process of verifying that approvals and procedures for recording and processing transactions have been obtained in accordance with management's general policies, standards, procedures, and specific instructions.

Autocratic leader
An autocratic leader is one who tends to centralize authority and rely on legitimate, reward, and coercive power to manage subordinates.

Autocratic management
(1) In autocratic management, managers are focused on developing an efficient workplace and have little concern for people. They typically make decisions without input from subordinates,

relying on their positional power. (2) Autocratic management conducted by a few key people who do not accept advice or participation from other employees

Autonomation
Autonomation is the automated shutdown of a production line, process, or machine upon detection of an abnormality or defect.

Availability
Availability is the state that exists when required automated services or system data can be obtained within an acceptable period at a level and in the form the system user wants.

Backbone
A backbone is a central network to which other networks connect.

Back door or trapdoor
A back door or trapdoor is a means of access to a computer program that bypasses security mechanisms.

Backflush
The term "backflush" means the deduction from inventory records of the component parts used in an assembly by exploding the bill of materials by the production count of assemblies produced.

Backup
A backup is a duplicate of a hardware system, of software, of data, or of documents intended as a replacement in the event of a malfunction or disaster.

Backup computer facility
A backup computer facility is a computer (data) center having hardware and software compatible with the primary computer facility. The backup computer is used only in the case of a major interruption or disaster at the primary computer facility. It provides the ability for continued computer operations, when needed, and should be established by a formal agreement.

Bandwidth
Bandwidth is the range of frequencies available to transmit signals. Hertz (cycles per second) is used to express the difference between the highest and lowest frequencies.

Barrier elements
Barrier elements inhibit the implementation and maintenance of various business programs and strategies.

Barriers to entrants
Barriers to entrants are any and all of the measures that a business can take to prevent potential competitors from entering the market.

Baseband
Baseband is a transmission technique in which devices can share a single communication channel. It is used in twisted-pair and coaxial cable media.

Baseline
A baseline is a set of critical observations or data used for a comparison or a control. It indicates a cut-off point in the design and development of a configuration item beyond which configuration does not evolve without undergoing strict configuration control policies and procedures.

Batch processing or patch mode
Batch processing or patch mode is the execution of a program or set of programs on the basis of a single initiating action. This method usually is run in the evenings or nights.

Baud
Baud is a measure of transmission speed. Baud and bits per second are equivalent. It measures the number of bits transmitted through a data channel in one second.

BCG matrix
A BCG matrix was developed by the Boston Consulting Group (BCG) that evaluates strategic business units with respect to the dimensions of business growth rate and market share.

Behaviorally Anchored Rating Scale (BARS)
BARS is a rating technique that relates an employee's performance to specific job-related incidents.

Benchmark
A benchmark is the measurement of performance against a uniform set of standards or environments.

Benchmark job
A benchmark job is a job found in many organizations and performed by several individuals who have similar duties that are relatively stable and require similar knowledge, skills, and abilities (KSAs).

Benchmarking
(1) Benchmarking is an improvement process in which a company measures its performance against that of best-in-class companies (or others that are good performers), determines how those companies achieved their performance levels, and uses the information to improve its own performance. The areas that can be benchmarked include strategies, operations, processes, and procedures. (2) "Benchmarking" means comparing specific measures of performance against data on those measures in other "best practice" organizations. (3) Benchmarking is the measurement of time intervals and other important characteristics of hardware and software, usually when testing them before a decision to purchase or reject. (4) Benchmarking is an ongoing, systematic approach by which a public affairs unit measures and compares itself with higher-performing and world-class units in order to generate knowledge and action about public affairs roles, practices, processes, products, services, and strategic issues that will lead to improvement in performance. Originated in the total quality management (TQM) movement.

Benefit-to-recipient standard
A benefit-to-recipient standard is a method for valuing subsidies by which the amount of the subsidy is determined in reference to a comparable commercial benchmark that would otherwise be available to the subsidy recipient within the jurisdiction in question.

Best practices
Best practices are the processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency.

Big Five personality factors
The Big Five personality factors are dimensions that describe an individual's extroversion, agreeableness, conscientiousness, emotional stability, and openness to experience.

Big Q, little q
"Big Q, little q" is a term used to contrast the difference between managing for quality in all business products and processes (Big Q) and managing for quality in only factory products and processes (little q). The difference is in the scope and size.

Bill of lading
A bill of lading is carrier's contract and receipt for goods it agrees to transport from one place to another and to deliver to a designated person. There are many types of bills of lading.

Bill of materials
A bill of materials is a list containing the quantity and description of all materials required to manufacture a single unit of a component or product. There are many types of bills of material.

Bill of sale
A bill of sale is a written document formally transferring ownership of property specified in the document from the supplier to the purchaser.

Bit
A bit is the smallest unit of information. A bit can represent two values, such as on/off, yes/no, true/false, or input/output.

Black box testing
Black box testing is a basic software test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. It examines the software from the user's viewpoint and determines if the data are processed according to the specifications. It does not consider implementation details. It verifies that software functions are performed correctly and that advertised security mechanisms are tested under operational conditions. It focuses on the external behavior of a system and uses the system's functional specifications to generate test cases. It ensures that the system does what it is supposed to do and does not do what it is not supposed to do. It is also known as generalized testing or functional testing, and should be combined with *white box testing* for maximum benefit because neither one by itself does a thorough testing job. Black box testing is functional analysis of a system.

Blacklisting
Blacklisting is the process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting also applies to (1) blocks placed against Internet Protocol addresses to prevent inappropriate or unauthorized use of Internet resources; (2) blocks placed on domain names known to attempt brute-force attacks; (3) a list of e-mail senders who have previously sent spam to a user; and (4) a list of discrete entities, such as hosts or applications, previously determined to be associated with malicious activity. Placing blacklisting and lifting blacklisting are both security-relevant events. Web content filtering software uses blacklisting to prevent access to undesirable Web sites.

Blanket order
A blanket order is a commitment to a supplier for certain goods over a predetermined period (one year) at predetermined prices or at prices to be determined.

Blasting, creating, and refining
Blasting, creating, and refining are used when a completely new way of thinking or speculation is required or when answering a question, such as "What else will do the job?" Blasting is good when group members are free to speculate and come up with totally new ideas that were never heard of or thought about before. Creativity comes into full play. It is a problem-solving tool.

Blocking
Blocking is the combining of two or more records into one block.

Blocking factor
A blocking factor is the number of records per block. A block is sometimes called a physical record, but this term is easily confused with logical record. Blocking is done for hardware efficiency and is unrelated to the way a user may wish to process data. The computer system usually handles all blocking and deblocking work automatically. Using efficient blocking factors can significantly improve input/output performance and use of storage space.

When allocating a data set, the blocking factor tells the computer what size groups of data to move at one time and what size groups of data to place on the storage device. Sound management practices dictate that system users should have their data blocked in as large a group as practicable for a given application.

Blue team

A blue team is a group of people conducting penetration tests. This team is responsible for defending an enterprise's use of information system by maintaining its security posture against a group of mock attackers (i.e., red team). The blue team must defend against real or simulated attacks (1) over a significant period of time, (2) in a representative operational context, and (3) according to rules established and monitored with the help of a neutral group (i.e., white team) refereeing the simulation or exercise.

Buffer overflow

Buffer overflow is a condition likely to occur in a programming interface under which more input is placed into a buffer or data-holding area than the capacity allocated, thus overwriting the information. Attackers and adversaries can exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. As a countermeasure, appropriate security controls should be used across operational, network, and host layers, combined with updated antivirus software and patches, firewalls, secure programming techniques, intrusion detection system software, and monitoring with security event management (SEM) tools. In addition, secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP) should be used instead of regular File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

Boot-sector virus

A boot-sector virus works during computer booting, where the master boot sector and boot sector code is read and executed. Such viruses place either their starting code or a jump to their code in the boot sector of floppies. They can also place the code either at the boot sector or at master boot sector of a hard disk. Most boot viruses infect by moving the original code of the master boot sector or boot sector to another location, such as slack space, and then by placing their own code in the master boot sector or boot sector. Boot viruses also infect the boot sector of floppy disks; some of them, such as Form, also infect the boot sector of hard disks. Other boot viruses infect the master boot sector of hard disks.

Botnet

Botnet is a term for a collection of software robots (bots) that run autonomously. A bot's originator can control the group remotely, usually through Internet relay chat, and usually for nefarious purposes. A botnet can comprise a collection of cracked computers running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command-and-control infrastructure. Botnets are often used to send spam e-mails and to launch denial-of-service attacks, phishing attacks, and virus attacks.

Bottleneck

A bottleneck is a facility, function, department, or resource whose capacity is less than the demand placed on it.

Bottom-up approach

A bottom-up approach starts with the lowest-level software components of a hierarchy and proceeds through progressively higher levels to the top-level component.

Bound tariff rates

Bound tariff rates are most-favored-nation (MFN) tariff rates resulting from General Agreement on Tariffs and Trade negotiations and thereafter incorporated as integral provisions of a country's schedule of concessions. The bound rate may represent a reduced rate or commitment not to raise the existing rate or a ceiling binding.

Brainstorming
Brainstorming is a technique to generate a great number of ideas. The key is to let group members feel free to express whatever ideas come to mind without fear of judgment or criticism. It is a problem-solving tool.

Bridge
A bridge is a device used to link two or more homogeneous local area networks. A bridge does not change the contents of the frame that is being transmitted but acts as a relay.

Broadband
Broadband is a transmission technique in which devices can communicate with each other on dedicated frequencies.

Browser
A browser is a client program used to interact on the World Wide Web.

Brute-force password attack
A brute-force password attack is a method of accessing an obstructed device by attempting multiple combinations of numeric and/or alphanumeric passwords, as found in simple passwords.

Budgeted capacity
Budgeted capacity is the volume/mix of throughput on which financial budgets were set and overhead absorption rates were established.

Buffer
A buffer is an area of random access memory or the central processing unit that is used to temporarily store data from a disk, communication port, program, or peripheral device.

Bug
A bug is an error or mistake in a computer program or data file.

Bureaucratic control
The term "bureaucratic control" refers to the use of rules, policies, hierarchy of authority, reward systems, and other formal devices to influence employee behavior and assess performance.

Bureaucratic organization
A bureaucratic organization is a subfield of the classical management perspective that emphasizes management on an impersonal, rational basis through such elements as clearly defined authority and responsibility, formal record keeping, and separation of management and ownership.

Bus
A bus is a topology in which stations are attached to a shared transmission medium.

Business ethics
Business ethics are concerned with good and bad or right and wrong behavior and practices that take place within a business context.

Business ethics gap
Compared with other capitalistic societies, the approach to ethics is more individualistic, legalistic, and universalistic in the United States.

Business ethics visibility gap
The people of the United States read and hear far more about business misconduct than people in other countries. Thus, there is a business ethics visibility gap in other countries.

Business-level strategy
Business-level strategy is the level of strategy concerned with the question "How do we compete?" It pertains to each business unit or product line within the organization.

Business market
The business marked is comprised of all organizations that buy goods and services for use in the production of other goods and services or for resale.

Business model
A business model is the manner in which businesses generate income.

Business necessity
A business necessity is a practice necessary for safe and efficient organizational operations.

Business partnering
Business partnering involves the creation of cooperative business alliances between constituencies within an organization or between an organization and its customers or suppliers. Partnering occurs through a pooling of resources in a trusting atmosphere focused on continuous, mutual improvement.

Business plan
A business plan is a document specifying the business details prepared by an entrepreneur in preparation for opening a new business.

Business planning
Business planning is the general idea or explicit statement of where an organization wishes to be at some time in the future.

Business processes
Business processes are processes that focus on what the organization does as a business and how it goes about doing it. A business has functional processes (generating output within a single department) and cross-functional processes (generating output across several functions or departments).

Business process reengineering
Business process reengineering is a systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes in order to achieve dramatic improvements in performance in areas important to customers and stakeholders.

Business report
A business report is a report that covers many of the matters typically found in the management discussion and analysis part of company annual reports in North America.

Business risk
Business risk is the possibility that a company will not be able to meet ongoing operating expenditures. It is the risk associated with projections of a firm's future returns on assets or returns on equity if the firm uses no debt.

Business stakeholder
A business stakeholder is a person or entity that has an interest in the economic performance of the business.

Business transaction
A business transaction occurrence is an economic event or a condition that must be recorded in the accounting records.

Buyback
A buyback is a type of countertrade in which a company builds a plant in a foreign country and agrees to take a certain portion of the plant's output as partial payment for the investment.

Buying (sourcing) team
A buying (sourcing) team is composed of individuals from several functional departments of a company who pool their expertise to jointly make sourcing decisions.

Byte
A byte is usually a group of eight bits. Bytes are the most convenient units for storing letters or characters, computer instructions, and system status indications.

C&E diagram
See Cause-and-effect diagram.

Cairns Group
The Cairns Group, established in August 1986, is an informal association of agricultural exporting countries. The group's members include Argentina, Australia, Brazil, Canada, Chile, Colombia, Hungary, Indonesia, Malaysia, New Zealand, the Philippines, Thailand, and Uruguay. Cairns Group countries account for one-third of world farm exports.

Call-back
A call-back is a procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

Call option
A call option is an option to buy a currency.

Canaries
Whereas honeypots analyze unauthorized connections, canaries flag that a connection attempt has taken place. Canaries provide passive network monitoring and work with network intrusion detection systems. Canaries can be stand-alone computers or unused network interface cards in existing hardware. Canaries complement intrusion detection systems.

Capacity
Capacity refers to the capability of a worker, machine, work center, plant, or organization to produce output per time period. Also, it is the capability of a system to perform its expected functions. Capacity can be classified in several ways, such as budgeted capacity, dedicated capacity, demonstrated capacity, productive capacity, protective capacity, excess capacity, idle capacity, rated capacity, safety capacity, and theoretical capacity.

Capacity strategy
Capacity strategy is a part of manufacturing (plant) strategy with three commonly recognized capacity strategies: lead, lag, and tracking. A lead strategy adds capacity in anticipation of increasing demand. A lag strategy does not add capacity until the firm is operating at or beyond full capacity. Both lead and lag capacity strategies are similar to the leading and lagging economic indicators.
A tracking strategy adds capacity in small amounts to or takes capacity away in small amounts to attempt to respond to changing demand in the marketplace. The tracking strategy is also called a level production strategy, where production is leveled with the demand.

$$\text{Lead capacity strategy} + \text{Lag capacity strategy} = \text{Chase capacity strategy}$$
$$\text{Tracking capacity strategy} = \text{Level production strategy}$$

All plant capacity strategies are related to demand in the marketplace.

Catalog
A catalog is systematic method of keeping track of stored data and programs in system libraries.

Cause-and-effect diagram (C&E diagram)
A C&E diagram (also called an Ishikawa or fishbone diagram), can be used to identify possible causes for a problem. The problem solver looks for the root causes by asking "why" five or six times to move from broad (possible) causes to specific (root) causes. The idea is that by repeating the same question, the true source of a problem will be discovered. This process helps identify the real problem. Then users choose the most likely cause for further review. Brainstorming can be used in developing the C&E diagrams.

Centralized multinational organizations
Centralized multinational organizations are those in which authority to make decisions is maintained at parent company headquarters.

Centralized network
A centralized network is a team communication structure in which team members communicate through a single individual to solve problems or make decisions.

Certification
Certification is a procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements. It is used in supplier certification and in issuing digital certificates.

Change management
Change management pertains to activities involved in (1) defining and instilling new values, attitudes, norms, and behaviors within an organization that support new ways of doing work and overcome resistance to change; (2) building consensus among customers and stakeholders on specific changes designed to better meet their needs; and (3) planning, testing, and implementing all aspects of the transition from one organizational structure or business process to another.

Channel
A channel is a path for electrical transmission between two or more connecting points. Also called path, link, line, or circuit.

Charismatic leader
A charismatic leader is one who has the ability to motivate subordinates to transcend their expected performance.

Chart and graph
The basic purpose of a chart or graph is to give a visual comparison between two or more things. For example, changes in budget from one year to the next may be represented in a graph. One significant reason for visualizing a comparison is to reinforce its comprehension. Charts and graphs are used to dramatize a statement, a fact, a point of view, or an idea. They are data presentation tools and visual aids assisting in the quick comprehension of simple and complex data, statistics, or problems. A chart should explain itself in silence; it should be completely understood without the assistance of a caption. The caption must act only as reinforcement to its comprehension.
Various charts include tabular charts, column charts, bar charts, pie charts, line charts, layer charts, and radar charts, as follows:

The **tabular chart** is used to represent items of interest. It requires a fair amount of study in order to grasp the full meaning of the figures. This is because it takes longer to digest the meaning of an itemization of compiled figures than if the same figures are presented graphically.

The **column chart** is most commonly used for demonstrating a comparison between two or more things. The column chart is vertical.

The **bar chart** or **Gantt chart** is essentially a column chart on its side, and is used for the same purpose. The bar chart is horizontal. It is a tool that allows a manager to evaluate whether existing resources can handle work demand or whether activities should be postponed. The Gantt chart is used for milestone scheduling where each milestone has start and completion dates. A milestone represents a major activity or task to be accomplished (e.g., design phase in a computer system development project). A **Gantt chart** is a graphical illustration of a scheduling technique. The structure of the chart shows output plotted against units of time. It does not include cost information. It highlights activities over the life of a project and contrasts actual times with projected times using a horizontal (bar) chart. It gives a quick picture of a project's progress in terms of actual time lines and projected time lines.

The **pie chart** is used to represent a 100% total of two or more items.

The **line chart** is very impressive when comparing several things but could present a visual problem if the comparisons are too many or too close in relation to one another. Advantages are that it is simple to draw. Disadvantages are that if the lines are close to each other, it is difficult to distinguish some of the plotted points.

The **layer chart** is linear in appearance but has a different representation. It depicts the accumulation of individual facts stacked one over the other to create the overall total. This chart is more complex than the others, since it illustrates much more. In addition to showing the comparison of layers that add up to the total, a layer chart also shows how each group of layers relates to subsequent groups. The layer chart requires more work to prepare than the other charts. There is more arithmetic involved, and it requires a good deal of concentration to draw the chart.

The **radar chart** is a visual method to show in graphic form the size of gaps in a number of areas, such as current performance versus ideal (expected) performance and current budget versus previous budget. Computer programs can be used to display radar charts.

Check digit
A check digit calculation helps ensure that the primary key or data are entered correctly.

Checklist
A checklist focuses one's attention on a logical list of diverse categories to which the problem could conceivably relate. It is a problem-solving tool.

Check-point
A check-point is a point, generally taken at regular intervals, at which a program's intermediate results are dumped to a secondary storage (e.g., disk) to minimize the risk of work loss.

Checksum
A checksum is an error-checking technique to ensure the accuracy of data transmission. The number of bits in a unit of data is summed and transmitted along with the data. The receiving computer then checks the sum and compares.

Chief knowledge officer (CKO)
The CKO is a relatively new position in some large organizations. The CKO is responsible for garnering knowledge and making it available for future operations in which employees can learn from previous experience. The CKO works closely with the chief information officer, who is in charge of the technical means for garnering the necessary information. In some firms, the position is called chief learning officer (CLO).

Chief learning officer (CLO)
The CLO is responsible for developing on a worldwide scale the organization's human talent and for using the human knowledge present in the organization. *See* Chief knowledge officer.

CIA triad
The CIA triad includes confidentiality, integrity, and availability, which are the primary objectives in information security.

Classical model
The classical model is a decision-making model based on the assumption that managers should make logical decisions that will be in the organization's best economic interests.

Clearing
Clearing is the removal of sensitive data from storage media at the end of a period of processing, including from peripheral devices with storage capacity, in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities (i.e., through the keyboard). Clearing may include use of advanced diagnostic utility programs. The storage media need not be disconnected from any external network before a clear. A potential risk is reconstruction of data if the clearing operation is not performed properly.

Click fraud
Click fraud involves deceptions and scams that inflate advertising bills with improper charges per click in an online advertisement on the Web. Advertisement firms hire several individuals to do repeat clicks in order to increase phony bills to their customers.

Client/server architecture
Client/server architecture is an architecture consisting of server programs that await and fulfill requests from client programs on the same or another computer.

Client/server authentication
Client/server authentication uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide client and server authentication and encryption of Web communications.

Closure
Closure is a perceptual process that allows a person to solve a complex problem with incomplete information. It is a problem-solving tool.

Cloud computing
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model promotes availability and is composed of five essential characteristics (i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (i.e., cloud software as a service, cloud platform as a service, and cloud infrastructure as a service), and four deployment models (i.e., private cloud, community cloud, public cloud, and hybrid cloud).

Coaching
Coaching is a continuous improvement technique by which people receive one-to-one learning through demonstration and practice. It is characterized by immediate feedback and correction.

Coaxial cable
Coaxial cable is an electromagnetic transmission medium consisting of a center conductor and an outer, concentric conductor.

Coercive power
Coerciver power is power that stems from the authority to punish or recommend punishment.

Cohesion
Cohesion is the degree to which the functions or processing elements within a module are related or bound together.

Cold site
A cold site is a backup, alternate computer processing location that have the basic infrastructure and environmental controls available (e.g., electrical, heating, and air conditioning) but no equipment or telecommunications established or in place. The cold site method is most difficult and expensive to test compared to the hot or warm site method. Cold sites are a part of information technology continuity planning.

Collective
In social interaction paradigm, leaders look for opportunities that benefit the group as a whole.

Collectivism
The term "collectivism" refers to: (1) a preference for a tightly knit social framework in which individuals look after one another and organizations protect their members' interests; or (2) the belief that interests of the organization should have top priority.

Collision
A collision is a condition in which two data packets are being transmitted over a medium at the same time from two or more stations.

Collision detection
When a collision is detected, in data transmission, the message is retransmitted after a random interval.

Commercial/industrial market
The term "commercial/industrial market" refers to business market customers who are described by variables such as location, Standard Industrial Classification (SIC) code, buyer industry, technological sophistication, purchasing process, size, ownership, and financial strength.

Common carrier
A common carrier serves all customers but carries only the types of freight for which it is certified.

Common cause
A common cause is a source of variation inherent in a process over time. It can affect every outcome of the process and everyone in the process.

Companion virus
A companion virus is a program that attaches to the operating system rather than files or sectors. In a disk operating system, when a user runs a file named "ABC," the rule is that ABC.COM would execute before ABC.EXE. A companion virus places its code in a .COM file whose first name matches the name of an existing .EXE. When a user runs the ABC file, the actual sequence of run is ABC.COM and ABC.EXE. In other words, a companion virus hides and spreads as a COM variant of a standard EXE file (e.g., clone war virus).

Comparative advantage
A comparative advantage results when a strategic advantage is held relative to the competition. The term also refers to a theory suggesting that specialization by countries can increase worldwide production. It is the ability to produce a good or service more cheaply, relative to other goods and services, than is possible in other countries.

Competence
Competence refers to a person's ability to learn and perform a particular activity. It generally consists of skill, knowledge, experience, and attitude components.

Competencies
Competencies are basic characteristics that can be linked to enhanced performance by individuals or teams.

Competitive advantage
Competitive advantage is defined as: (1) A position in which one dominates a market; also called strategic advantage. (2) The ability to produce a good or service more cheaply than other countries due to favorable factor conditions and demand conditions; strong related and supporting industries; and favorable firm strategy, structure, and rivalry conditions.

Competitive analysis
Competitive analysis involves the gathering of intelligence relative to competitors in order to identify opportunities or potential threats to current and future strategy.

Competitive assessment
Competitive assessment is a research process that consists of matching markets to corporate strengths and providing an analysis of the best potential for specific offerings.

Competitive disadvantage
The Trade-Related Investment Measures (TRIMs) agreement contains a provision concerning "competitive disadvantage." This provision would allow countries to apply existing TRIMs to new investing firms for the duration of the transition period when (1) the products of such investment were similar to the products of the established enterprises and (2) it was necessary to avoid distorting the conditions of competition between the new investment and the established enterprises.

Competitive environment
A competitive environment is affected by bribery and the existence of cartels.

Competitively advantaged product
A competitively advantaged product is a product that solves a set of customer problems better than any competitor's product. This product is made possible due to a firm's unique technical, manufacturing, managerial, or marketing capabilities, which are not easily copied by others.

Communications software
Communications software is a program that moves electronic messages from computer to terminals and vice versa.

Compensating control
The compensating control concept states that the total environment should be considered when determining whether a specific policy, procedure, or control is violated or a specific risk is present. If controls in one area are weak, they should be compensated for or mitigated in another area. Some examples of compensating controls are: strict personnel hiring procedures, bonding employees, information system risk insurance, increased supervision, rotation of duties, review of computer logs, user sign-off procedures, mandatory vacations, batch controls, user review of input and output, system activity reconciliations, and system access security controls.

Compiler
A compiler is a program that translates a source code module (statements written in a human readable programming language) to computer-readable machine language, and produces an object code module.

Compliance
The term "compliance" refers to verifying that both manual and computer processing of transactions or events are in accordance with the organization's policies and procedures, generally accepted accounting principles, governmental laws, and regulatory agency rules and requirements.

Compliance testing
Compliance testing is the process of verifying compliance with the organization's internal controls, operations, policies, plans, procedures, guidelines, practices, and standards to evaluate efficiency and effectiveness. The process is called compliance auditing, and the tests performed are called compliance tests.

Compulsory licensing
Compulsory licensing is an authorization by a government that permits someone, without the consent of the patent owner, to make, use, or sell a patented product; or to use a patented process; or to use, sell, or import the product produced by a patented process. Compulsory licenses are granted by governments for many reasons, among them to permit local production of a product if the patent owner is not "working" (i.e., manufacturing the product) the patent in the country within a specified period of time or to allow a patent holder to exploit the patent that, absent a license, would infringe on an earlier granted patent.

Concentration strategy
Concentration strategy is a market development strategy that involves focusing on a smaller number of markets.

Configuration accounting
The recording and reporting of configuration item descriptions and all departures from the baseline during design and production.

Configuration auditing
Configuration auditing is an independent review of computer software for the purpose of assessing compliance with established requirements, standards, and baseline.

Configuration control
Configuration control is the process of controlling modifications to the system's design, hardware, firmware, software, and documentation, thus providing sufficient assurance that the system is protected against the introduction of improper modification prior to, during, and after system implementation.

Configuration identification
Configuration identification is the identifying of the system configuration throughout the design, development, test, and production tasks.

Configuration item
A configuration item is the smallest component of hardware, software, firmware, documentation, or any of its discrete portions, that is tracked by the configuration management system.

Configuration management
Configuration management is management of security features and assurances through control of changes made to hardware, software, firmware, documentation, and actual test with test data and results throughout the life cycle of an information system.

Consideration
Consideration is a type of leader behavior that describes the extent to which a leader is sensitive to subordinates, respects their ideas and feelings, and establishes mutual trust.

Consignment buying
Consignment buying is a method of procurement in which a supplier maintains inventory on the purchaser's premises. The purchaser's obligation to pay for the goods begins when goods are drawn from the stock for use.

Constructed value
Constructed value is a means of determining fair or foreign market value when sales of the specific or the similar merchandise do not exist or, for various reasons, cannot be used for comparison purposes. In U.S. antidumping law, the constructed value consists of (1) the cost of materials and fabrication or other processing employed in producing the merchandize, (2) the general expense of not less than 10% of material and fabrication costs, and (3) a profit of not less than 8% of the sum of the production costs and general expenses.

Contention
Contention it is a state of busy condition between a terminal and a channel. If the channel in question is free, transmission is done. Otherwise, the terminal waits. Also, it is the condition when two or more stations attempt to use the same channel at the same time.

Contingency plan
A contingency plan is a plan that includes procedures for storing hardware, software, supplies, and personnel to operate the backup computer facilities in the case of a major interruption or disaster at the primary computer facility. Also called disaster recovery plan, business resumption plan, or business continuity plan.

Continuous process improvement
Continuous process improvement is an ongoing effort to incrementally improve how products and services are provided and internal operations are conducted.

Contract carrier
Tariff rates do not apply to contract transportation services, and contract rates will be lower than common carrier rates.

Control
A control is any protective action, device, procedure, technique, or other measure that reduces exposure. Controls can prevent, detect, or correct errors, forms of loss or harm.

Control language
Control language consists of statements that introduce a computer job to the system and, among other things, specify input/output file requirements, storage space requirements, space allocation requirements, releasing the storage space not needed after the job has ended, and blocking factors. An example is job control language in an IBM environment.

Control unit
A control unit is an electrical device that connects an input/output (I/O) device to a channel. I/O devices are connected to the central processing unit through channels and control units.

Cookies
Cookies are small text files on a computer that store information about what Web sites a user accessed while browsing the Internet. They are used to track a user across multiple Web sites. Cookies are used for storing user authentication data. Cookies combined with Web bugs are used to build user profiles. Often information collected with cookies is sold to third parties. Four types of cookies exist: persistent, session, tracking, and encrypted, as follows:

A **persistent cookie** is stored on a computer's hard drive indefinitely so that a Web site can identify the user during subsequent visits. These cookies are set with expiration dates and are valid until the user deletes them.

A **session cookie** is a temporary cookie that is valid only for a single Web site session. It is stored in temporary memory and is erased when the user closes the Web browser.

A **tracking cookie** is placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior.

Encrypted cookies are created by Web sites to protect the data from unauthorized access.

Cooperative purchasing
Cooperative purchasing is a volume-buying approach in which several organizations form or utilize a centralized buying service that purchases specified types of items for all members of the group.

Coordinated decentralization
Coordinated decentralization involves headquarters providing the overall corporate strategy while granting subsidiaries the freedom to implement it within established ranges.

Copybook
A copybook is a file that contains the source code that can be directly copied into a program by reference. It also contains program segments, edit/validation routines, and global tables.

Core competence
Core competence is: (1) a business activity that an organization does particularly well in comparison to competitors; (2) a unique capability that creates high value and that differentiates the organization from its competition.

Core dump
A core dump is a printout or display of an image of a computer memory or an area that is suspended from further processing. It can be used as a program debugging tool.

Core processes
Core processes have a major impact on the strategic goals of an organization.

Corporate charter
A corporate charter is a document filed with the secretary of the state in which the firm is incorporated that provides information about the company, including its name, address, directors, and amount of capital stock.

Corporate culture
The term "corporate culture" refers to: (1) the collective beliefs, values, attitudes, manners, customs, behaviors, and artifacts unique to an organization; (2) an organization's practice, such as its symbols, heroes, and rituals; and its values, such as its employees' perception of good/evil, beautiful/ugly, normal/abnormal, and rational/ irrational. The practice aspects differ from corporation to corporation within a national culture, and the value aspects vary from country to country.

Corporate governance
Corporate governance is the method by which a firm is being governed, directed, administered, or controlled and to the goals for which it is being governed. Corporate governance is concerned with the relative roles, rights, and accountability of such stakeholder groups as owners, boards of directors, managers, employees, and others who assert to be stakeholders.

Corporate-level strategy
The corporate-level strategy is the strategy concerned with the question "What business are we in?" It pertains to the organization as a whole and the combination of business units and product lines that make it up.

Corrective maintenance
The term "corrective maintenance" refers to changes to software necessitated by actual errors in a system.

Cost, insurance, and freight (CIF)
CIF is a sales practice in international trade in which the supplier quotes a price that includes the cost of the material, freight charges to a destination point, and marine insurance en route.

Cost of production
Cost of production refers to the sum of the cost of materials, fabrication, and/or other processing employed in producing the merchandise sold in a home market or to a third country, together with appropriate allocations of general administrative and selling expenses. The cost of production is based on the producer's actual experience and does not include any mandatory minimum general expenses or profit, as in "constructed value."

Copyright
A copyright is a property right in an original work of authorship that arises automatically upon creation of such a work and belongs, in the first instance, to the author.

Cost/benefit analysis
Cost/benefit analysis is a decision-making tool in which the expected costs and benefits of alternative actions are compared. The action for which the expected value of the benefits minus the expected value of the costs is greatest is chosen. The expected value is the desirability of alternative multiplied by the probability of success. The likelihood of an occurrence that is derived mathematically from reliable historical data is called objective probabilities. However, subjective probabilities do not have mathematical reliability since they are derived from the decision maker's intuition and gut feel of.

Cost leadership
Cost leadership is a: (1) pricing tactic where a company offers an identical product or service at a lower cost than the competition; (2) type of competitive strategy with which the organization aggressively seeks efficient facilities, cuts costs, and employs tight cost controls to be more efficient than competitors.

Counterfeiting
Counterfeiting refers to the unauthorized and deliberate duplication of another's trademarks and patents.

Counterpurchase
A counterpurchase is a form of countertrade that occurs when a firm agrees to purchase a specified dollar volume of materials from a country in return for a sale made to that country.

Countertrade
Countertrade is a general term used for any type of transaction that requires, as a condition of the original sale, that goods be bought either as a trade-balancing mechanism or as full or partial payment for the goods sold.

Countervailing duty
A countervailing duty is a special duty imposed by an importing country to offset the economic effect of a subsidy and thus prevent injury to a domestic industry caused by a subsidized import.

Coupling
The term "coupling" refers to the degree to which modules in a computer program depend on each other.

Credit memo
A credit memo is a document used to correct an overcharge, pay a rebate, or credit the value of goods returned.

Cryptography
Cryptography is the only known current practical means of securing data and information that are transmitted over communications lines such as cable, microwave, fiber optics, or satellite.

Cultural barriers
Business behavior in one culture does not transfer well to another culture due to cultural differences. For example, Americans' competitive culture does not transfer well to cooperative cultures, such as Japan.

Cultural environment
To develop an effective international business strategy, the critical aspects of culture must be identified.

Cultural fluency
Cultural fluency refers to a strong command of not only the language of a foreign country but also its culture. This is required for effective cross-cultural communication.

Cultural imperialism
Criticism by some that the United States is forcing its products and culture on other cultures through technological advances and the globalization of business.

Cultural leader
A cultural leader is a manager who uses signals and symbols to influence corporate culture.

Cultural relativism
Cultural relativism is the belief that no culture's ethics are any better than any other's.

Cultural risk
Cultural risk is the risk of business blunders, poor customer relations, and wasted negotiations that results when firms fail to understand and adapt to the differences between their own and host countries' cultures.

Cultural universals
Cultural universals are manifestations of the total way of life of any group of people.

Culture
Culture: (1) comprises an entire set of social norms and responses that condition people's behavior; it is acquired and inculcated, a set of rules and behavior patterns that an individual learns but does not inherit at birth; (2) system of values, beliefs, and behaviors inherent in an organization or society. *See* Corporate culture.

Culture free
A theory proposing that managerial behavior is affected by specific situations in all cultures.

Culture gap
Culture gap is the difference between an organization's desired cultural norms and values and actual norms and values.

Culture shock
The term "culture shock" refers to the more pronounced reactions to the psychological disorientation that most people feel when they move for an extended period of time to a markedly different culture. It is what expatriates experience after the novelty of living in a new culture wears out.

Culture shock phase
The culture shock phase, the third phase in the expatriation process, usually begins two months into the disillusionment phase. After two months of day-to-day confusion, the expatriate wishes to go back to his or her old, familiar environment.

Culture specific
A theory proposing that managerial behavior is affected by a nation's culture.

Cumulation
Under the practice of cumulation, the effects of imports from several sources are combined to determine the existence of injury to a domestic industry. Cumulative assessment of injury can occur when imports from many sources compete simultaneously with each other and a domestic industry and where all of the imports are subject to dumping or countervailing duty investigations.

Currency Swap
A currency swap is an agreement to trade currencies at one date and reverse the trade at a later date. It is a financial market.

Cut-off
A cut-off is a process of verifying that all transactions are recorded in the proper accounting period to protect and provide consistency of input data and output results (based on specific beginning and ending dates).

Cycle checker
In a database systems or programs a cycle checker detects and resolves deadlocks.

Cycle count
A cycle count is a physical stock-checking system in which the inventory is divided into groups, one of which is physically counted each week.

Cycle time
Cycle tyime represents the time interval between initiating a transfer of data to or from storage and the instant when this transfer is completed. Same as execution time.

Cyclic redundancy check (CRC)
In CRC, an algorithm is used to generate error detection bits in a data link protocol. The receiving station performs the same calculation as done by the transmitting station. If the results differ, then one or more bits are in error.

Database
A database is a collection of interrelated data stored together, using a common and controlled approach.

Database system
In a database system, data are maintained independently of the application programs. Data can be shared by many programs and users. Database management system (DBMS) software manages and controls the data and the database software.

Data dictionary
A data dictionary contains attributes and characteristics of each data element or field in a computer record. It also includes file organization and structure and edit and validation rules.

Data Encryption Standard (DES)
DES is an encryption standard established by the National Bureau of Standards. The use of DES or some other encryption algorithm is essential for securing telecommunications.

Data remanence
Data remanence is residual data remaining on storage media after clearing. It is a residual risk.

Data set
Data set is a term referring to a collection of related bytes, or characters, of secondary storage. For example, a data set may be a file of payroll records or a library of payroll programs.

Deadlock
A deadlock is a consequence of poor resource management that occurs when two programs each control a resource (e.g., printer, data file, and record) needed by the other and neither is willing to give in its resource.

Debugging
Debugging is the process of correcting mistakes or errors in a computer program.

Decipher
The term "decipher" means to convert, by use of the appropriate key, enciphered text into its equivalent plain text.

Decision table
A decision table is a decision-making tool that documents rules used to select one or more actions based on one or more conditions. These conditions and their corresponding actions can be presented either in a matrix or tabular form.

Decision tree
A decision tree is a graphical representation of possible decisions, events, or states of nature resulting from each decision with its associated probabilities, and the outcomes of the events or states of nature. The decision problem displays the sequential nature of the decision-making situation. The decision tree has nodes, branches, and circles to represent junction boxes, connectors between the nodes, and state-of-nature nodes, respectively. It is a decision-making tool.

Decrypt
To decrypt is to convert, by use of the appropriate key, encrypted (encoded or enciphered) text into its equivalent plaintext.

Dedicated capacity
Dedicated capacity is designated to produce a single item or a limited number of similar items.

Defense in breadth
Defense in breadth is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). It is a strategy dealing with scope of information protection coverage of a system. Also called supply chain protection control, it supports an agile defense strategy.

Defense in depth
Defense in depth is an information protection strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of information systems. It is an approach for establishing an adequate information assurance (IA) posture whereby (1) IA solutions integrate people, technology, and operations; (2) IA solutions are layered within and among IT assets; and (3) IA solutions are selected based on their relative level of robustness. Implementation of this approach recognizes that the highly interactive nature of information systems and enclaves creates a shared risk environment; therefore, the adequate assurance of any single asset is dependent on the adequate assurance of

all interconnecting assets. It is an information protection strategy dealing with controls placed at multiple levels and at multiple places in a given system. It supports agile defense strategy and is same as security in depth.

Degaussing
Degaussing, also called demagnetizing, is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field to magnetic media.

Deleted file
A deleted file has been logically, but not physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data, which is an easy target for an electronic scavenging attack.

Delphi technique
The Delphi technique is a method used to avoid groupthink in which group members do not meet face to face to make decisions. Rather, each group member independently and anonymously writes down suggestions and submits comments, which are then centrally compiled. The compiled results are then distributed to the group members who, independently and anonymously, write additional comments. These comments are again centrally compiled, and the process is repeated until consensus is obtained. The Delphi technique is a problem-solving tool and a group decision-making method.

Demand-pull system
A demand-pull system is a material movement technique where a downstream work center pulls materials from the upstream work center when they are needed, not when on a schedule.

Demilitarized zone (DMZ)
A DMZ is an interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. DMZ is a host or network segment inserted as a neutral zone between an organization's private network and the Internet. It is a network created by connecting to firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.

De minimis dumping or subsidy level
De minimis dumping is the level below which a dumping margin or subsidy is considered to be negligible. Antidumping or countervailing duty actions are terminated in cases where the margin of dumping or level of subsidy is below the de minimis level.

Demonstrated capacity
Demonstrated capacity is a proven capacity calculated from actual performance data. It is expressed as the average number of items produced multiplied by the standard hours per item.

Dependent demand
Dependent demand refers to the demand for an item that is derived from the demand for another component or a finished product.

Detailed design
Detailed design is a process where technical specifications are translated into more detailed programming specifications, from which computer programs are developed.

Devil's advocate technique
In the devil's advocate technique, the decision maker is focusing on failures and identifies ways an action or an alternative can be less than successful. It is a decision-making tool.

Differential analysis
Differential analysis is a technique to compare differences in revenues or costs of two or more alternatives. It is a decision-making tool.

Digital certificate
A digital certificate is a password-protected and encrypted file that contains identification information about its holder. It includes a public key and a unique private key.

Digital signature
Digital signature is electronic information stored or transferred in digital form. It is a nonforgeable transformation of data that allows the proof of the source (with nonrepudiation) and the verification of the integrity of that data. Digital signatures provide authentication and integrity protection.

Digital watermarking
Digital watermarking is the process of irreversibly embedding information into a digital signal to hide sensitive data.

Direct Access Storage Device (DASD)
DASD is a migration device (disk) that transfers files to tape or cartridge in order to efficiently use file space.

Direct investing
Direct investing is: (1) an entry strategy in which the organization is involved in managing its production facilities in a foreign country; (2) an established operations in a country.

Direct investment account
A direct investment account is an account in the balance of payment (BOP) statement that records investments with an expected maturity of more than one year and an investor's ownership position of at least 10%.

Direct involvement
Direct involvement is participation by a firm in international business in which the firm works with foreign customers or markets to establish a relationship.

Directory
A directory is the list of files stored on a disk.

Discount rate
A discount rate is the interest rate at which member banks can borrow from the Federal Reserve Banks. It is a cost of borrowing to member banks.

Discretionary access control (DAC) policy
The basis for a DAC policy is that an individual user or program operating on the user's behalf is allowed to specify explicitly the types of access other users or programs executing on their behalf may have to the information under the user's control. DAC is called a surrogate access control. *Compare* with mandatory access control policy.

Discriminant analysis
Discriminant analysis is a qualitative, subjective decision-making tool to differentiate between effective and ineffective procedures or actions.

Diseconomies of scale
Diseconomies of scale explain a phenomenon where a plant expanding over time results in higher per unit costs. As the plant capacity reaches its maximum levels.

Disk array
Disk array is a recovery control technique used to improve the performance of data storage media regardless of the type of computer used. Disk arrays use parity disk schema to keep track of data stored in a domain of the storage subsystem and to regenerate it in case of a hardware/software failure. Disk arrays use multiple disks. If one disk drive fails, the other one becomes available. They also have six levels from level zero through five (i.e., Redundant Array of Independent Disks [RAIDs]). They use several disks in a single logical subsystem. Disk arrays are also called *disk striping*.

Disk duplexing
The purpose of disk duplexing is same as with disk arrays. The disk controller is duplicated. When one disk controller fails, the other one is ready to operate.

Disk farm
A disk farm is data that are stored on multiple disks for reliability and performance reasons.

Disk mirroring
The purpose of disk mirroring is the same as with disk arrays. A file server contains two physical disks and one channel, and all information is written to both disks simultaneously (disk-to-disk copy). If one disk fails, all of the data are immediately available from the other disk. Disk mirroring uses a copy/image technique to make an identical copy of the hard drive. It incurs some performance overhead during write operations and increases the cost of the disk subsystem since two disks are required. Disk mirroring should be used for critical applications that can accept little or no data loss. This is a technical and recovery control and ensures availability goal. It is synonymous with disk shadowing.

Disk replication
Disk replication is data that are written to two different disks to ensure that two valid copies of the data are always available. It minimizes the time for recovery.

Disk striping
Disk striping contains more than one disk and more than one partition, and is same as *disk array*s. An advantage of disk striping is running multiple drives in parallel. A disadvantage is that its organization is more complicated than disk farm and is highly sensitive to multiple failures.

Diversionary dumping
Diversionary dumping occurs when foreign producers sell to a third-country market at less than fair value and the product is then further processed and shipped to another country.

Domestication
Domestication refers to government demand for partial transfer of ownership and management responsibility from a foreign company to local entities, with or without compensation.

Domestic enterprises
Domestic enterprises are companies that derive all of their revenues from their home market.

Domestic environment
The domestic environment refers to home country factors, including the political, competitive, economic, and legal and governmental climates, that affect an enterprise.

Division
A division is decentralized organizational unit that is structured around a common function, product, customer, or geographical territory. Divisions can be cost, profit, or investment centers.

Divisional structure
Divisional structure is an organization structure in which departments are grouped based on similar organizational outputs.

Driver
A driver is program code that sets up an environment and calls a module for testing.

Dual cable
In dual cable systems, two separate cables are used: one for transmission and one for reception.

Dual control
Dual control in information technology is the process of utilizing two or more separate entities or two individuals operating in concert to protect sensitive functions or information. No single entity is able to generate, access, or use cryptographic keys. This is similar to dual control in physical access, such as opening a safe vault in the presence of two individuals. All entities are equally responsible. This approach generally involves the split knowledge of the physical or logical protection of security parameters.

Dump
A dump is a process of copying or printing the contents of computer program, central processing unit memory, or data file to find errors and to conduct analysis.

Dumping
Dumping is the sale of a commodity in a foreign market at a lower price than its fair market value. Dumping is generally recognized as unfair because the practice can disrupt markets and injure producers of competitive products in an importing country. Both the General Agreement on Tariffs and Trade and the World Trade Organization permit imposition of antidumping duties equal to the difference between the price sought in the importing country and the normal value of the product in the exporting country.

Dumping margin
The dumping margin is the amount by which the imported merchandise is sold in the United States below the home market or third-country price or the constructive value (i.e., at less than its fair value). For example, if the U.S. purchase price is $200 and the fair value is $220, the dumping margin is $20. This margin is expressed as a percentage of the U.S. price. In this example, the margin is 10% ($20/$200).

Duty
A duty is a tax imposed on imports by the customs authority of a country. Duties are generally based on the value of the goods (ad valorem duties), some other factors such as weight or quantity (specific duties), or a combination of value and other factors (compound duties).

Dynamic gains
Dynamic gains increase the rate of economic growth. Even a small change in the growth rate can lead to a substantial cumulative effect on gross domestic product. Thus, empirical assessment of the dynamic effects of trade policy changes can yield substantially larger estimates than those based on static models. The growth effects of trade liberalization can flow through a variety of channels, such as improved access to specialized capital goods, human capital accumulation, learning by doing, transfer of skills, and new product introduction.

Dynamic risk
Dynamic risk, in contrast to static risk, is produced because of changes in society. Dynamic risks also can be either pure or speculative. Examples of sources of dynamic risk include urban unrest, increasingly complex technology, and changing attitude of legislatures and courts about a variety of issues.

Easter egg
An Easter egg is a form of computer virus that triggers when a program code is placed in software for the amusement of its developer or users. It is a nuisance to users.

Eavesdropping
Several definitions of eavesdropping exist. It is: (1) Passively monitoring network communications for data and authentication credentials; (2) the unauthorized interception of information-bearing emanations through the use of methods other than wiretapping; and (3) a passive attack in which an attacker listens to a private communication. The best way to thwart this attack is by making it very difficult for an attacker to make any sense of the communication by encrypting all messages. Eavesdropping is also known as packet snarfing.

Economies of scale
Economies of scale mean: (1) achievement of lower average cost per unit by means of increased production; and (2) production economies made possible by the output of larger quantities. They explain the downward sloping of the long-run average total cost curve. As the size of a plant increases, its average costs of production decreases due to several factors.

Economies of scale and economies of scope
These economies are obtained by spreading the costs of distribution over a large quantity of products (scale) or over a wide variety of products (scope).

Edisonian
Edisonian is a type of trial-and error experimentation named after Thomas Edison. This method requires a tedious and persistent search for the solution. It is a problem-solving tool.

Effectiveness
(1) The degree to which the organization achieves a stated goal. **(2)** The measure of how well a job is performed.

Efficiency
Efficiency is a measurement (usually expressed as a percentage) of the actual output to the standard output expected. Efficiency measures how well something is performing relative to existing standards; in contrast, productivity measures output relative to a specific input, for example, tons/labor hour. Efficiency is the ratio of (1) actual units produced to the standard rate of production expected in a time period or (2) standard hours produced to actual hours worked (taking longer means less efficiency) or (3) actual dollar volume of output to a standard dollar volume in a time period. Illustrations of these calculations follow.

There is a standard of 100 pieces per hour and 780 units are produced in one eight-hour shift; the efficiency is 780/800 converted to a percentage, or 97.5%.

The work is measured in hours and took 8.21 hours to produce eight standard hours; the efficiency is 8/8.21 converted to a percentage, or 97.5%.

The work is measured in dollars and produces $780 with a standard of $800; the efficiency is $780/$800 converted to a percentage, or sense that the price reflects all publicly available information on each security.

Eighth Directive of the European Union
The European Union (EU) Eighth Directive deals with auditing of financial statements of companies in EU countries and specifies that they be consistent with EU law. It also sets qualifications for auditors and the firms conducting audits, including education and experience requirements. In addition, the directive deals with ethical matters, such as independence, and includes sanctions for cases in which audits are not conducted as prescribed by statute.

Embargo
An embargo is the most restrictive barrier to exporting to a country, often resulting from political actions.

Emulate
To emulate is to use firmware to allow original code to run on target hardware, with no functional change.

Encipher
To encipher is to convert plaintext into unintelligible form by means of a code system.

Encrypt
To encrypt is to convert plaintext into unintelligible form by means of a cryptographic system.

Encrypted virus
An encrypted virus has two parts: a small decryptor and the encrypted virus body. When the virus is executed, the decryptor executes first and decrypts the virus body. Then the virus body executes by replicating or becoming resident. The virus body includes an encryptor to apply during replication. A variably encrypted virus uses different encryption keys or encryption algorithms. Encrypted viruses are more difficult to disassemble and study since the researcher must decrypt the code. The variably encrypted virus code begins with a decryption algorithm and continues with the scrambled or encrypted code of the remainder of the virus. When several identical files are infected with the same virus, they share a brief identical decryption algorithm but, beyond that, each copy may appear different. A scan string can be used to search for the decryption algorithm.

Enterprise-level strategy
An enterprise-level strategy is the overarching strategy level that poses these basic questions: "What is the role of the organization in society?" and "What do we stand for?"

Enterprise Risk Management (ERM) program
Traditionally, corporate risk management focused on partial portfolio of risks (silo approach), specifically on financial and hazard risks. This narrow scope ignored all the other risks impacting the organization. It did not exploit the natural hedges and portfolio effects in the collective and tended to treat risk as downside phenomenon.
An ERM program focuses on total portfolio risks, including financial, hazard, strategic, and operational risks. The scope of ERM is much broader than the traditional view with the objective of creating, protecting, and enhancing shareholder value. ERM treats risk as both upside and downside phenomenon since it integrates all risks. Scorecards, action plans, and monitoring are part of the ERM approach.

Enterprise-wide resource planning (ERP) system
An ERP is a system that integrates enterprise-wide information, including human resources, finance, manufacturing, and distribution, and connects the organization to its customers and suppliers.

Ethical dilemma
A ethical dilemma is a situation that arises when all alternative choices or behaviors have been deemed undesirable because of potentially negative ethical consequence, making it difficult to distinguish right from wrong.

Ethical impact statement
An ethical impact statement is an attempt to assess the underlying moral justifications for corporate actions and the consequent results of those actions.

Ethical relativism
Ethical relativism refers to picking and choosing which source of norms to use based on what will justify current actions or maximize freedom.

Ethical responsibilities
Ethical responsibilities are those activities and practices that are expected or prohibited by societal members even though they are not codified into law.

Ethical values
Ethical values are moral values that enable a decision maker to determine an appropriate course of behavior; these values should be based on what is right, which may go beyond what is legal.

Ethical vigilance
Ethical vigilance involves paying constant attention to whether one's actions are right or wrong and, if ethically wrong, asking why one is behaving in that manner.

Ethics
Ethics is a: (1) code of conduct that is based on moral principles and that tries to balance what is fair for individuals with what is right for society; (2) code of moral principles and values that govern the behaviors of a person or group with respect to what is right or wrong; (3) discipline that deals with what is good and bad and with moral duty and obligation.

Ethnocentric
The word "ethnocentric" refers to tending to regard one's own culture as superior; tending to be home-market oriented.

Ethnocentric staffing outlook
The ethnocentric staffing outlook is the belief that key positions in foreign subsidiaries should be staffed by citizens from the parent company's home country.

Ethnocentric strategy
In an ethnocentric strategy, companies produce unique goods and services that they offer primarily to their domestic market. When they export, they do not modify the product or service for foreign consumption.

Ethnocentrism
Ethnocentrism is a cultural attitude marked by the tendency to regard one's own culture as superior to others; the belief that one's own group or subculture is inherently superior to other groups or cultures.

Ethnorelativism
Ethnorelativism is the belief that groups and subcultures are inherently equal.

European Free Trade Agreement (EFTA)
EFTA is a regional trade group established in 1958 by the Treaty of Stockholm and originally comprised of Denmark, Sweden, Norway, the United Kingdom, Austria, Portugal, Switzerland, Finland, and Iceland. The United Kingdom, Portugal, and Denmark have since left EFTA to join the European Union. EFTA has mainly been concerned with the elimination of tariffs with respect to manufactured goods originating in the EFTA countries and traded among them.

European Union (EU)
The EU is a supranational legal regime with its own legislative, administrative, treaty-making, and judicial procedures. To create this regime, several European nations have surrendered substantial sovereignty to the EU.

Excess capacity
Excess capacity is where the output capabilities at a nonconstraint resource exceed the amount of productive or protective capacity required to achieve a given level of throughput at the constraint.

Execution time
See Cycle time.

Existence
The term "existence" refers to a process of verifying that the assets, liabilities, and other documents are real. Also, it refers to the actual existence of documentation (systems, program, computer operations, help-desk, network control, and user), software, and data.

Expatriate
An expatriate is: (1) an employee working in an operation who is not a citizen of the country in which the operation is located but is a citizen of the country of the headquarters organization; (2) an employee who lives and works in a country other than his or her own.

Expatriation
Expatriation involves preparing and sending global employees to their foreign assignments.

Expatriation program
An expatriation program takes place while the expatriate is working in the foreign operations; certain delivery and communications programs are required.

Expectancy theory
Expectancy theory is a process theory that proposes that motivation depends on individuals' expectations about their ability to perform tasks and receive desired rewards.

Expert power
Expert power is power that stems from special knowledge of or skill in the tasks performed by subordinates.

Export complaint system
An export complaint system allows customers to contact the original supplier of a product in order to inquire about products, make suggestions, or present complaints.

Export control system
A export control system is a system designed to deny or at least delay the acquisition of strategically important goods to adversaries; in the United States, it is based on the Export Administration Act and the Munitions Control Act.

Export-Import Bank (Ex-Im Bank)
The Ex-Im Bank is a bank that attempts to strengthen the competitiveness of U.S. industries involved in foreign trade.

Exporting
Exporting is an entry strategy in which the organization maintains its production facilities within its home country and transfers its products for sale in foreign markets.

Exporting restriction
An exporting restriction limits company exports, or sales for export, by placing a restriction on a particular product, a volume or value of products, or a proportion of the volume or value of the company's local production.

Export license
An export license is a license obtainable from the U.S. Department of Commerce Bureau of Export Administration, which is responsible for administering the Export Administration Act.

Export management company (EMC)
An EMC is a domestic firm that specializes in performing international business services as commissioned representatives or as distributors.

Export subsidy
An export subsidy is generally a subsidy that is provided on the basis of export performance.

Export trading company (ETC)
The result of 1982 legislation to improve the export performance of small and medium-size firms, the ETC allows businesses to band together to export or offer export services. Additionally, the law permits bank participation in trading companies and relaxes antitrust provisions.

Expropriation
Expropriation refers to government takeover of a company's operations frequently at a level lower than the value of the assets.

External economies of scale
External economies of scale are lower production costs resulting from the free mobility of factors of production in a common market.

Extrinsic reward
An extrinsic reward is a reward given by another person.

Extranet
An extranet is the Internet technology is used to connect the intranet of an organization with the intranet from other organizations, such as suppliers and customers.

Failover
Failover is: (1) the capability to switch over automatically without human intervention or warning to a redundant or standby information system upon the failure or abnormal termination of the previously active system; (2) a backup concept in that when the primary system fails, the backup system is automatically activated. It is related to information technology.

Fail-safe
A fail-safe is an automatic protection of programs and/or processing systems when hardware or software failure is detected in a computer system. It is a condition to avoid compromise in the event of a failure or have no chance of failure. It is related to information technology.

Fail-safe default
A fail-safe default asserts that access decisions should be based on permission rather than exclusion. This equates to the condition in which lack of access is the default, and the protection scheme recognizes permissible actions rather than prohibited actions. Also, failures due to flaws in exclusion-based systems tend to grant (unauthorized) permissions, whereas permission-based systems tend to fail-safe with permission denied. It is related to information technology.

Fail-secure
In a fail-secure system, the system preserves a secure condition during and after an identified failure. It is related to information technology.

Fail-soft
A fail-soft is a selective termination of affected nonessential processing when hardware or software failure is determined to be imminent in a computer system. The computer system continues to function because of its resilience. Fail-soft methods are found in distributed data processing systems. They are related to information technology.

Fail-stop processor
A fail-stop processor is one that can constrain the failure rate and protects the integrity of data. However, it is likely to be more vulnerable to denial-of-service attacks. It is related to information technology.

Failure
Failure is a discrepancy between external results of a program's operation and software product requirements. A software failure is evidence of software faults. It is related to information technology.

Failure access
Failure access is a type of incident in which unauthorized access to data results from hardware or software failure. It is related to information technology.

Failure control
Failure control is a methodology used to detect imminent hardware or software failure and provide fail-safe or fail-soft recovery in a computer system. It is related to information technology.

Failure costs
Failure costs are associated with evaluating and either correcting or replacing defective products, components, or materials that do not meet quality standards. Failure costs can be either internal, occurring prior to the completion or shipment of a product or the rendering of a service, or external, occurring after a product is shipped or a service is rendered. Examples of internal failure costs include repair, redesign, reinspection, rework, retesting, sorting, and scrap. Examples of external failure costs include product warranty charges, returns, and recalls; liability suits; and field service staff training costs. Failure costs are associated with poor quality of products or services.

Failure rate
The failure rate is the number of times the hardware ceases to function in a given time period. It is related to information technology.

Fallback procedure
A fallback procedure refers to the ability to: (1) fall back to the original or alternate method for continuation of processing in the event of a failure of transactions or the system; (2) go back to the original or alternate method for continuation of computer processing. It is related to information technology.

Feasibility study
A feasibility study determines whether the needs of system users can be satisfied by a system's solution, considering the cost, capabilities, and benefits in developing, acquiring, operating, and maintaining a computer system.

Fault-tolerance mechanisms
Fault-tolerance mechanisms have the built-in capability to provide continued, correct execution of their assigned functions in the presence of hardware and/or software faults. Examples of such mechanisms include disk mirroring, server mirroring, disk duplexing, block mirroring, and check-pointing. Check-pointing is needed before, during, or after completion of critical transactions or events to ensure acceptable fault recovery.

Femininity
Femininity refers to: (1) a cultural preference for cooperation, group decision making, and quality of life; (2) the quality of life, nurturing, and relationships.

File
A file is a collection of related records.

File allocation table
A table, stored on disk, containing an entry for each cluster on the disk.

File infector virus
A file infector virus attaches itself to (or replaces) .COM and .EXE files, although in some cases it can infect files with extension .SYS, .DRV, .BIN, .OVL, .OVR, and others. The most common file infector viruses are resident viruses, going into memory at the time the first copy runs and taking clandestine control of the computer. Such viruses commonly infect additional programs as they are run. Nonresident viruses simply infect one or more files whenever an infected file is run.

File organization
The term "file organization" refers to the manner in which records in a computer data file appear and are accessed for data entry, update, processing, retrieval, and query purposes (i.e., sequential, direct access).

File server
A file server sends and receives data between a workstation and the server.

File transfer protocol (FTP)
FTP is an Internet standard for transferring files over the Internet. It is a means to exchange files across a network. FTP programs and utility programs are used to upload and download Web pages, graphics, and other files between local media and a remote server that allows FTP access. For example, in smart phones, the FTP server could result in arbitrary code execution, which is risky. Use of FTP is risky since it uses a weak security protocol.

Financial engineering
The goal of financial engineering is to reduce financial risks that, its goals are achieved through financial instruments, such as derivative securities (e.g., hedging with forward contracts). Financial engineering can also be applied to insurance and reinsurance areas using alternate risk transfer methods (e.g., captive insurance) as part of a company's risk mitigation strategy. In a way, financial engineering is related to risk engineering in terms of sharing common goals, such as risks, hedging, insurance, and captive insurance.

Financial risk
A financial risk is a risk arising from volatility in foreign currencies, interest rates, and commodities. It includes credit risk, liquidity risk (bankruptcy risk), interest rate risk, and market risk.

Firewall
A firewall is a method of protecting a network against security threats from other systems and networks by centralizing and controlling access to the network using a combination of hardware and software controls. Several definitions exist for a firewall: (1) A process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer; security domains are established that require authorization to enter. (2) A product that acts as a barrier to prevent unauthorized or unwanted communications between sections of a computer network. (3) A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. (4) A gateway that limits access between networks in accordance with local security policy. (5) A system designed to prevent unauthorized accesses

to or from a private network. Firewalls often are used to prevent Internet users from accessing private networks connected to the Internet.

Firmware
The term "firmware" refers to computer programs and data loaded in a class of memory that cannot be easily modified by the user during processing.

Fiscal drag
Fiscal drag is a possibility of an economy operating at a high level of employment, resulting in surpluses that can be contractionary in nature.

Fishbone diagram
A fishbone diagram is a graphic technique for identifying cause-and-effect relationships among factors in a given situation or problem. It is also called Ishikawa diagramming.

Fit-gap analysis
Fit-gap analysis is a technique that compares a company's existing state to its desired state (as expressed by its long-term plans) to determine what fits and what does not fit (gap) and what needs to be done to remove or minimize the gap. Examples include (1) a gap between service providers' and service receivers' expectations, (2) a gap between supplier/vendor's goals and customer's goals, (3) a gap between business strategies and business processes, and (4) a gap between a computer's CPU performance and data storage subsystem performance.

Fixed-order quantity system
A fixed-order quantity system is one in which the order quantity is fixed and the time between orders varies.

Float
Float is an amount of money represented by checks outstanding and in the process of collection.

Flowchart
A flowchart helps a decision maker in analyzing a large, complex problem. Flowcharts and decision trees both show flow or sequencing. Unlike the flowchart, a decision tree shows outcome probabilities. It is a problem-solving and decision-making tool.

Force-field analysis
Force-field analysis involves the identification of a problem, the factors or forces contributing to making it a problem, and steps for generating solutions. Two main sets of forces are identified: (1) inhibiting forces—those that resist the resolution of the problem; and (2) facilitating forces—those that push the problem toward resolution. It is a problem-solving tool.

Foreign Corrupt Practices Act (FCPA)
FCPA is an established U.S. code of conduct making it illegal for U.S. businesses to bribe foreign government officials, political parties, and political candidates, even if it is an acceptable practice in the foreign country. It also requires appropriate accounting controls for full disclosure of firms' foreign transactions.

Foreign direct investment
Foreign direct investment is: (1) an international entry strategy that is achieved through the acquisition of foreign firms or (2) the establishment or expansion of operations of a firm in a foreign country. Like all investments, it assumes a transfer of capital.

Foreign environment
The term "foreign environment" refers to factors in a country that affect international business, including the country's cultural, legal, political, competitive, economic, and technological systems.

Foreign exchange balancing
Foreign exchange balancing restricts a company's imports by limiting the company's access to foreign exchange to pay for goods to some proportion of the amount of foreign exchange earned by the company.

Foreign investment
Many countries' laws dictate that foreign investments in their nation must be in the form of a joint venture with local partners and that the local partners must be majority owners.

Foreign market opportunity analysis
Foreign market opportunity analysis is broad-based research to obtain information about the general variables of a target market outside a firm's home country.

Foreign policy
Foreign policy is the area of public policy concerned with relationships with other countries.

Foreign service premium
A foreign service premium is a financial incentive to accept an assignment overseas, usually paid as a percentage of the base salary.

Foreign subsidiary
A foreign subsidiary is an international firm's operating unit established in foreign countries. It typically has its own management structure.

Foreign tax credit
A foreign tax credit is credit applied to home-country tax payments due for taxes paid abroad.

Foreign trade zone
A foreign trade zone is a special area where foreign goods may be held or processed without incurring duties and taxes.

Forward buying
Forward buying means buying in excess of current requirements as part of strategy or because of anticipated shortages, strikes, or price increases.

Forward logistics versus reverse logistics
In forward logistics, raw materials and finished products are moved from upstream suppliers to downstream customers. In reverse logistics, already sold finished products are moved from the downstream customers to upstream suppliers and eventually to manufacturers for returns and repairs.

Forward market
A forward market is a financial market that buys and sells currencies to be delivered at a future date.

Fragmentation
Fragmentation refers to chunks of unused space throughout primary memory or secondary storage device.

Frame
A frame is a group of bits that include data plus one or more addresses. It is the unit of data that is handled by the data link level layer (layer 2) of software in a data communication system.

Franchising
Franchising is: (1) a form of licensing in which an organization provides its foreign franchisees with a complete assortment of materials and services; an arrangement by which the owner of a product or service allows others to purchase the right to distribute the product or service

with help from the owner; (2) a form of licensing that allows a distributor or retailer exclusive rights to sell a product or service in a specified area; (3) an agreement by which a firm provides specialized sales or service strategy, support assistance, and possibly an initial investment in the franchise in exchange for periodic fees; (4) a form of licensing that grants a wholesaler or a retailer exclusive rights to sell a product or a service in a specified area.

Free alongside (FAS) vessel
In a FAS vessel, the supplier agrees to deliver the goods in proper condition alongside the vessel. The buyer assumes all subsequent risks and expenses after delivery to the port or pier.

Free on board (FOB)
FOB is a contractual arrangement in which title is transferred between supplier and purchaser at the FOB point. There are many variations of FOB.

Free trade area
A free trade area is an area in which all barriers to trade among member countries are removed, although sometimes only for certain goods or services.

Full duplex
A full duplex data communication line can transmit in both directions at once.

Functional design
Functional design is a process in which the user's needs are translated into a system's technical specifications.

Functional-level strategy
A functional-level strategy addresses the question: How should a firm integrate its various sub-functional activities, and how should these activities be related to changes taking place in the various functional areas? The strategy pertains to all of the organization's major departments.

Functional organization
A functional organization is structured by discrete functions (e.g., marketing/sales, engineering, production, finance, human resources).

Functional organization structure
Functional organization structure is an organizational structure in which groups are made up of individuals who perform the same function, such as engineering or manufacturing, or have the same expertise or skills, such as electronics engineering or testing.

Functional structure
Functional structure is an organization structure in which positions are grouped into departments based on similar skills, expertise, and resource use.

Futures contract
A futures contract is used for the purchase or sale and delivery of commodities at a future date. It is primarily used as a hedging device against market price fluctuations or unforeseen supply shortages.

Gainsharing
Gainsharing is a type of program that rewards individuals financially on the basis of organizational performance.

Gantt chart
A Gantt chart is a project management technique to pictorially represent the tasks to be performed and the interrelationships among tasks in a project. It is also called a bar chart. It shows the time frame (e.g., hours, days) for each task.

Gap-fit analysis
Gap-fit analysis is a technique that compares a company's existing state to its desired state (as expressed by its long-term plans) to determine what fits and what does not fit (gap) and what needs to be done to remove or minimize the gap. Examples include (1) a gap between service providers' and service receivers' expectations, (2) a gap between supplier/vendor's goals and customer's goals, (3) a gap between business strategies and business processes, and (4) a gap between a computer's CPU performance and data storage subsystem performance.

Gateway
A gateway is a device to connect two different networks.

General Agreement on Tariffs and Trade (GATT)
GATT was created in 1947 as an interim measure pending the establishment of the International Trade Organization (ITO), under the Havana Charter. The ITO was never ratified by the U.S. Congress. Operating in the absence of an explicit international organization, GATT has provided the legal framework for international trade, with its primary mission being the reduction of trade barriers.

General Agreement on Trade in Services (GATS)
GATS is a set of international rules governing trade and investment in the services sector. It is the first multilateral, legally enforceable agreement covering trade and investment in the services sector. For the first time, services would be subject to many of the same rules that cover trade in goods. The GATS framework, however, is structured somewhat differently from GATT itself. For example, market access and national treatment are not automatically provided for, as they are in GATT. These two principles would become binding commitments only in services sectors that countries schedule in bilateral negotiations under the GATT's auspices.

General semantics
General semantics includes approaches that help individuals to discover multiple meanings or relationships in words and expressions. It is a problem-solving tool.

Generalized System of Preferences (GSP)
GSP is a program under which the United States grants duty-free treatment to selected imports from designated beneficiary developing nations and territories. The program began in 1976, when the United States joined with other members of the Organization for Economic Cooperation and Development (OECD) to promote the economic growth and development of developing countries.

Geocentric staffing outlook
A geocentric staffing outlook holds that nationality should not make any difference in the assignment of key positions anywhere (local subsidiary, regional headquarters, or central headquarters); that competence should be the prime criterion for selecting managerial staff.

Geographic organization
A geographic organization is one structured by geography, territory, region, and so on.

Global
Global refers to worldwide interdependencies of financial markets, technology, and living standards.

Global account management
Global customers of a company may be provided with special services including a single point of contact for domestic and international operations and consistent worldwide service.

Global capital markets
Global capital markets are those markets in a global economy that attract investors and investees from throughout the world.

Global corporate culture
Global corporate culture is the core values that cut across all of a firm's subsidiaries located around the globe.

Global corporations
Global corporations are international businesses that view the world as their marketplace.

Globalization
Globalization: (1) refers to the global economic integration of many formerly national economies into one global economy; (2) is the notion that in the future, more and more companies will have to conduct their business activities in a highly interconnected world, thus presenting their management with the challenge of reengineering systems to cope with this new environment. Globalization involves awareness, understanding, and response to global developments as they affect a company; (3) is the standardization of product design and advertising strategies throughout the world.

Globalization approach
A globalization approach is an approach to international marketing in which differences are incorporated into a regional or global strategy that will allow for differences in implementation.

Global manager
A global manager is an international executive with the ability to manage enterprises in diverse cultures.

Global mind-set
In today's global environment, even for employees who may not go abroad, it is necessary to constantly sensitize everyone to the notion that the company is in a global business.

Global organization
A global organization is one having corporate units in a number of countries integrated to operate worldwide.

Global outsourcing
Global outsourcing is engaging in the international division of labor so as to obtain the cheapest sources of labor and supplies regardless of country; also called global sourcing.

Global Reporting Initiative
The Global Reporting Initiative is an international, multistakeholder effort to create a common framework for voluntary reporting of the economic, environmental, and social impact of organization-level activity.

Global strategy
A corporation using a global strategy uses all of its resources against its competition in a very integrated fashion—all of its foreign subsidiaries and divisions are highly interdependent in both operations and strategy.

Global team
A global team is a work team made up of members of different nationalities whose activities span multiple countries; may operate as a virtual team or meet face to face.

Global village
"Global village" is a term used to refer to our world in the age of information and telecommunications because people are highly accessible to each other.

Glocalization
Glocalization is: (1) a term coined to describe the networked global organization approach to an organizational structure; (2) the planning and designing of global Web sites so that they also cater to local needs and preferences.

Goal
A goal is a: (1) desired future state that the organization attempts to realize; (2) statement of general intent, aim, or desire; it is the point toward which management directs its efforts and resources; goals are often nonquantitative.

Goal conflict
Goal conflict occurs when an employee's self-interest differs from business objectives.

Gopher
Gopher is a protocol designed to allow a user to transfer text or binary files among computer hosts across networks.

Grand strategy
A grand strategy is the general plan of major action by which an organization intends to achieve its long-term goals.

Grapevine
The grapevine consists of informal communication channels over which information flows within an organization, usually without a known origin of the information and without any confirmation of its accuracy or completeness (sometimes referred to as the rumor mill).

Graphic rating scale
A graphic rating scale is a scale that allows the rater to mark an employee's performance on a continuum.

Gray box testing
Gray box testing is a software test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. It is also known as focused testing.

Gray market
A gray market is a market entered in a way not intended by the manufacturer of the goods.

Gray marketing
Gray marketing is the marketing of authentic, legally trademarked goods through unauthorized channels.

Grease payments
Grease payments are minor, facilitating payments to officials for the primary purpose getting them to do whatever they are supposed to do anyway.

Greenfield venture
A greenfield venture is the most risky type of direct investment, whereby a company builds a subsidiary from scratch in a foreign country.

Greenmail
The term "greenmail" refers to a situation in which a firm, trying to avoid a takeover, buys back stock at a price above the existing market price from the person(s) trying to gain control of the firm.

Grey area measures
Grey area measures involve actions countries take outside the General Agreement on Tariffs and Trade (GATT) or World Trade Organization (WTO) safeguard laws to address import

surges. Such measures include voluntary restraint agreements, quotas, tariff increases, and agreements among countries to trade specific goods at specific prices.

Group of Seven
The Group of Seven includes the United States, Canada, the United Kingdom, France, Germany, Italy, and Japan representing the world's major industrial countries.

Half-duplex
A half-duplex data communication line can transmit in both directions, but only in one direction at a time.

Halo effect
The halo effect is an overall impression of a person or situation based on one characteristic, either favorable or unfavorable; a type of rating error that occurs when an employee receives the same rating on all dimensions regardless of his or her performance on individual ones.

Harmonized formula approach
The harmonized formula approach applies a formula to cut high tariff rates, called peak tariffs, by a greater percentage than applied to low tariffs. Thus, the goal is to lower tariffs and to achieve more consistent tariff levels among contracting parties.

Hazard
Hazard is a condition that creates or increases the probability of a loss. Three types of hazards exist: (1) physical hazard, (2) moral hazard, and (3) morale hazard. Physical hazard is a condition of the subject of insurance that creates or increases the chance of loss, such as structural defects, occupancy, or similar conditions. Moral hazard is a dishonest predisposition on the part of an insured that increases the chance of loss. Morale hazard is a careless attitude on the part of an insured that increases the chance of loss or causes losses to be greater than would otherwise be the case.

Hazard risk
A hazard risk is a risk that is insurable, such as natural disasters, various insurable liabilities, impairment of physical assets and property, and terrorism.

Hedge or hedging
Hedge or hedging is taking a position opposite to the exposure or risk. This can be done with financial derivatives, such as futures contracts, forward contracts, options, and swaps. A perfect hedge is not possible because financial derivatives used to hedge do not move together, leaving some risk. The idea behind hedging is to minimize risk. A value is created for shareholders if corporate hedging does not duplicate the shareholders' "homemade" hedging.

Hedging operation
A hedging operation is done through matching the liability created by borrowing foreign currencies with the asset created by lending domestic currency, both to be repaid at the known future exchange rate.

High-context culture
A high-context culture is one in which in which behavioral and environmental nuances are an important means of conveying information. In the course of business, participants establish social trust first, value personal relations and goodwill, make agreements on the basis of general trust, and like to conduct slow and ritualistic business negotiations.

High-power distance culture
In a high-power distance culture, a person at a higher position in the organizational hierarchy makes the decision and the employees at the lower levels simply follow the instructions.

Honeypot systems
Honeypot systems are decoy systems that attempt to lure an attacker away from critical systems. These fake production systems are filled with information that is seemingly valuable but that has actually been fabricated and would not be accessed by an honest user. Thus, when access to the honeypot is detected, there is a high likelihood that it is an attacker. The purpose of the honeypot is to divert an attacker from accessing critical systems, collecting information about the attacker's activity, and encouraging the attacker to stay on the system long enough for a security administrator to respond. Honeynet is a network of honeypots designed to attract hackers so that their intrusions can be detected and analyzed. It is important to consult with the legal department before deploying a honeypot or honeynet for any legal ramifications of monitoring an attacker's activity. Honeypots or honeynets complement intrusion detection systems.

Horizontal analysis
Horizontal analysis is financial analysis that compares an item in a current statement with the same item in prior statements.

Horizontal communication
Horizontal communication is the lateral or diagonal exchange of messages among peers or coworkers.

Horizontal dependency
Horizontal dependency is the relationship between the components at the same level in the bill of material, in which all must be available at the same time and in sufficient quantity to manufacture the parent assembly.

Horizontal information interchange
Horizontal information interchange means sharing information by organizations in a horizontal market.

Horizontal market
A horizontal market is a market in which all players buy or sell the same type of product, making them competitors.

Horizontal merger
A horizontal merger is a combination of two firms that produce the same type of good or service.

Horizontal promotion
In a horizontal promotion, instead of slowly climbing the organizational ladder, a worker or manager makes lateral movements, acquiring expertise in different functions, such as marketing or manufacturing.

Horizontal structure
A horizontal structure is an organization that is organized along a process or value-added chain, eliminating hierarchy and functional boundaries (also referred to as a systems structure).

Horizontal team
A horizontal team is a formal team composed of employees from about the same hierarchical level but from different areas of expertise.

Hoshin planning
Hoshin planning is a type of Japanese strategic planning process in which an organization develops up to four vision statements that indicate where the organization should be in the next five years. Company goals and work plans are developed based on the vision statements. Periodic audits are then conducted to monitor progress. It is a breakthrough planning process.

Host-country national
A host-country national is an employee working for a firm in an operation who is a citizen of the country where the operation is located, but the firm's headquarters are in another country.

Hostile environment
A hostile environment involves harassment, where an individual's work performance or psychological well-being is unreasonably affected by intimidating or offensive working conditions.

Hostile takeover
A hostile takeover is the acquisition of a company over the opposition of its management.

Hot site
A hot site is a backup, alternate computer processing location with fully operational equipment and capacity to quickly take over system operations after loss of the primary system facility. A hot site has sufficient equipment and the most current version of production software installed, and adequate storage for the production system data. A hot site is used for short-term needs while a cold site is used for long-term needs. Hot sites are a part of information technology continuity planning.

House of quality
A house of quality is a structured process that relates customer-defined attributes to the product's technical features needed to support and generate these attributes. It is part of the quality function deployment process and forces designers to consider customer needs and the degree to which the proposed designs satisfy these needs. It is also called voice of the customer, where the term "customer" indicates the external customer of the supplying entity.

Humor
In addition to being a powerful tool to relieve tension and hostility, humor is a problem-solving tool. When correctly executed, it opens the mind to seeking creative solutions to the problem. Humor can be in the form of detached jokes, quips, games, puns, and anecdotes. Humor gives perspective and solves problems. Stepping back and viewing a problem with a certain level of detachment restores perspective. A sense of humor sends messages of self-confidence, security, and control of the situation. However, humor should not be sarcastic or scornful.

Hygiene factors
Hygiene factors are: (1) factors that involve the presence or absence of job dissatisfiers, including working conditions, pay, company policies, and interpersonal relationships; (2) a term used by Frederick Herzberg to label "dissatisfiers."

HyperText Markup Language (HTML)
HTML is a mechanism used to create Web pages on the Internet.

HyperText Transport Protocol (HTTP)
HTTP is the native protocol of the Web, used to transfer hypertext documents on the Internet.

Identity-based access control (IBAC) policy
IBAC policy is an access control mechanism based only on the identity of the subject and object. An IBAC decision grants or denies a request based on the presence of an entity on an access control list. Identity-based access controls and discretionary access control are considered equivalent.

Idle capacity
Idle capacity is the capacity not used in a system of linked resources. It consists of protective capacity and excess capacity.

Imagineering
Imagineering is a problem-solving tool that involves the visualization of a complex process, procedure, or operation with all waste eliminated. The imagineer assumes the role of dreamer, realist, and critic. The steps in imagineering consist of taking an action, comparing the results with the person's imagined perfect situation, and making mental correction for the next time. This approach eventually improves the situation and brings it to the desired level. Imagineering is similar to value analysis.

Impersonation
Impersonation is an attempt to gain access to a system by posing as an authorized user.

Importing and exporting
Importing and exporting refer to buying and selling goods and services with organizations in other countries.

Import substitution
An import substitution policy is a policy for economic growth adopted by many developing countries that involves the systematic encouragement of domestic production of goods formerly imported.

Independent testing of software
Independent testing of software is conducted by an independent accredited software testing organization as per the ISO/IEC 17025 standard to verify that it meets both functional requirements and software quality assurance requirements. The testing organization can use either a white box or black box scenario, depending on the need.

Index
An index is a secondary path to data. Indexes are normally used to enhance the speed of data retrieval at the expense of update speed.

Individualism
Individualism: (1) is a preference for a loosely knit social framework in which individuals are expected to take care of themselves; (2) is a dimension of culture that refers to the extent to which people in a country prefer to act as individuals instead of members of groups; (3) is the trait in which the employee attaches higher importance to personal and family interests than to the organization; (4) refers to the degree to which people in a society look after primarily their own interests or belong to and depend on in groups.

Individualism approach
An individualism approach is the ethical concept that acts are moral when they promote the individual's best long-term interests, which ultimately leads to the greater good.

Informal communication
Informal communication is unofficial communication that takes place in an organization as people talk freely and easily; examples include impromptu meetings and personal conversations (verbal or e-mail).

Informal communication channel
An informal communication channel is a communication channel that exists outside formally authorized channels without regard for the organization's hierarchy of authority.

Informal integration
Informal integration allows a foreign subsidiary to adopt the corporation's global vision, core values, and cultural principles in its own way. That is, the corporation's central management does not formally force these on the foreign subsidiaries; rather, it listens to people at the local level and communicates with them.

Information engineering
Information engineering (IE) is an approach to planning, analyzing, designing, and developing an information system with an enterprise-wide perspective and an emphasis on data and architectures.

Information system
An information system (IS) is the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems include financial, nonfinancial, and mixed systems.

Information technology (IT)
IT is the hardware and software operated by an organization to accomplish a function, regardless of the technology involved (e.g, computers, telecommunications, etc.).

Information technology (IT) architecture
IT architecture is an integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the organization's strategic goals. A complete IT architecture should consist of both logical and technical components. The logical architecture provides the high-level description of the organization's mission, functional requirements, information requirements, system components, and information flows among the components. The technical architecture defines the specific IT standards and rules that will be used to implement the logical architecture.

Initial program load (IPL)
IPL is the process of reading the resident operating system into computer main, central processing unit, primary memory.

Initialize
The term "initialize" refers to the process of clearing computer storage areas, addresses, or memory in the beginning of a program routine or job startup.

Initiator
An initiator is IBM's term for a transient module that starts and ends tasks. Also called terminator.

Insurable interest
An insurable interest is an interest that might be damaged if the peril insured against occurs; the possibility of a financial loss to an individual or a corporation that can be protected against through insurance.

Insurance
Insurance is an economic risk transfer mechanism whereby an individual or a corporation substitutes a small certain cost (the premium) for a large uncertain financial loss (the claim, or contingency insured against) that would exist if it were not for the insurance policy (contract). Insurance is most appropriate for situations in where there is a low frequency and a high severity of occurrence.

Integrated international operation
An integrated international operation is a foreign operation whose economic activities have a direct impact on the reporting (parent) entity.

Intellectual property (IP) rights
Patents, trademarks, and copyrights are three primary forms of IP rights in worldwide use. Other types of IP rights include trade secrets, mask works, and industrial designs (i.e., the ornamental aspect of a useful article).

Interactive leadership
Interactive leadership is a leadership style characterized by values such as inclusion, collaboration, relationship building, and caring.

Internal economies of scale
Internal economies of scale are lower production costs resulting from greater production for an enlarged market.

International competitiveness
International competitiveness is the ability of a firm, an industry, or a country to compete in the international marketplace at a stable or rising standard of living.

International contracts
International contracts involve additional issues beyond those in domestic contracts, such as differences in language, legal systems, and currency.

International corporation
An international corporation is an international business that produces products in its home country and exports to other countries.

International Court of Justice (ICJ)
The ICJ is the judicial branch of the United Nations having voluntary jurisdiction over nations.

International division
An international division is a unit established to supervise a firm's exports and its foreign distribution agreements, sales forces, sales branches, and subsidiaries.

International human resource management function
An international human resource management function consists of interplay among three dimensions: the broad function, country categories, and types of employees.

International intermediaries
International intermediaries are marketing institutions that facilitate the movement of goods and services between the originator and customer.

Internationalization
Internationalization is a process by which firms increase their awareness of the influence of international activities on their future and establish and conduct transactions with firms from other countries.

International labor relations
The term "international labor relations" refers to the management of a multinational corporation interacting with organized labor units in each country.

International law
International law includes law that deals with the conduct and relations of nation-states and international organizations as well as some of their relations with persons; such law is enforceable by the courts of a nation that has adopted the international law as domestic law.

International management
International management is the management of business operations conducted in more than one country.

International marketing
International marketing is the process of planning and conducting transactions across national borders to create exchanges that satisfy the objectives of individuals and organizations.

International organizational structure
The firm's organizational structure is its "skeleton"; it provides support and ties together disparate functions.

International organizations
The term "international organizations" refers to groupings of nations (such as the European Union), worldwide bodies (such as the World Bank), organizations of nations by industry (such as the Organization of Petroleum Exporting Countries), and the World Trade Organization.

International pricing
International pricing is a managerial decision about what to charge for goods produced in one nation and sold in another.

International product life cycle (IPLC)
IPLC is a theory that many products that are exported to foreign countries are eventually produced abroad and that foreign producers subsequently obtain a competitive edge over the original producers, forcing them to either create a new product or go out of business.

International relocation and orientation
International relocation and orientation involves making arrangements for predeparture training, immigration and travel details, and finalizing compensation details between the expatriate and the home country.

International Trade Commission (ITC)
ITC is an independent federal government agency that conducts statutory trade-related investigations and studies and reports on a wide range of international trade and economic policy issues for the U.S. president and Congress.

Internet
The Internet is the worldwide network of networks that use the transmission control protocol/internet protocol (TCP/IP) protocol suite for communications.

Internetworking
Internetworking is communication among devices across multiple networks.

Interpreter
An interpreter is the same as *compiler*, in a computer software, but an interpreter translates on single source statement and executes those machine-level instructions and then moves on to the next source statement.

Intranet
The Internet technology is used to develop a network within an organization for communicating among and between employees.

Intrusion detection system (IDS)
An IDS is a computer security system to detect, report, and provide a limited response to a security incident that may be harmful to an information system.

Intrusion prevention system (IPS)
An IPS provides security policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide preventive action upon being alerted. IPS and IDS should be combined with a firewall for a stronger protection.

Intuitive approach
The intuitive approach is a problem-solving tool based on hunches. It does not use a scientific approach and uses subjective estimates or probabilities, which are difficult to replicate.

Investigative questions
Six investigative questions are used to understand the root causes of issues and problems better: who, what, when, where, why, and how. The questions are a problem-solving tool.

Java
Java is a programming language invented by Sun Microsystems. It can be used to as a general-purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets. The execution environment for Java applets is intended to be safe (i.e., executing an applet should not modify anything outside the World Wide Web browser).

Jidoka
Jidoka is the practice of stopping the production line when a defect occurs. It is a Japanese term.

Job accounting system
A job accounting system is software that provides job start and completion times; user, program, and data file identification; and usage of datasets. This information can be used to charge functional users for the computer resources they consume.

Job analysis
Job analysis is a systematic way to gather and analyze information about the content, context, and human requirements of jobs.

Job characteristics model
The job characteristics model is a model of job design that comprises core job dimensions, critical psychological states, and employee growth-need strength.

Job criteria
Job criteria are important elements in a given job.

Job design
Job design is: (1) the application of motivational theories to the structure of work for improving productivity and satisfaction; (2) organizing tasks, duties, and responsibilities into a productive unit of work.

Job description
A job description is a narrative explanation of the work, responsibilities, and basic requirements of a job.

Job enlargement
Job enlargement is a job design that combines a series of tasks into one new, broader job to give employees variety and challenge.

Job enrichment
Job enrichment is: (1) a job design that incorporates achievement, recognition, and other high-level motivators into the work; (2) increasing the depth of a job by adding the responsibility for planning, organizing, controlling, and evaluating the job.

Job evaluation
Job evaluation is the process of determining the value of jobs within an organization through an examination of job content.

Job management
Job management involves routines that dispatch, enqueue, schedule, initiate, and terminate jobs or tasks.

Job name
A job name is the name chosen by the programmer to identify a job.

Job rotation
Job rotation is a job design that systematically moves employees from one job to another to provide them with variety and stimulation.

Job satisfaction
Job satisfaction is a positive emotional state resulting from evaluating one's job experience.

Job scheduling
Job scheduling is an orderly scheduling of production jobs that brings discipline to a computer operations department and reduces panic and last-minute rush situations. When combined with data input cut-off procedures, it provides consistency from one accounting period to another.

Job simplification
Job simplification is a job design whose purpose is to improve task efficiency by reducing the number of tasks a single person must do.

Job specifications
Job specifications are the knowledge, skills, and abilities (KSAs) an individual needs to perform a job satisfactorily.

Job statement
A job statement is a statement used to separate and identify jobs.

Job step
A job step is a single program in a job.

Job stream
A job stream series of computer jobs submitted, in batch mode, to the operating system. The job stream holds control statements, source code, and data. It is a job grouping of tasks, duties, and responsibilities that constitutes the total work assignment for employees.

Joint venture
Joint venture: (1) two or more firms that band together to establish operations in foreign markets in order to capitalize on each other's resources and reduce risk. They share profits, liabilities, and duties; (2) result from the participation of two or more companies in an enterprise in which each party contributes assets, owns the new entity to some degree, and shares risk.

Journal
A journal is an audit trail of system activities. It is useful for file/system recovery purposes.

Joystick
A joystick is a sticklike pointing device that can be used to indicate the speed and direction of cursor movement to the central processing unit.

Kaizen
Kaizen is a Japanese term that refers to continuous improvement involving everyone in the company. In manufacturing, it relates to finding and eliminating waste in machinery, labor, or production methods.

Kanban
Kanban is a method of just-in-time production that uses standard containers or lot sizes with a single card attached to each. It is a Japanese term.

Kerberos
Kerberos is an authentication tool used in local logins, remote authentication, and client/server requests. It is a means of verifying the identities of principals on an open network. Kerberos accomplishes this without relying on the authentication, trustworthiness, or physical security of hosts while assuming all packets can be read, modified, and inserted at will. Kerberos uses a trust broker model and symmetric cryptography to provide authentication and authorization of users and systems on the network.

Kernel virus
A kernel is the base of an operating system of a computer system. A kernel virus loads into memory ahead of the operating system and avoids many traditional forms of virus detection. The virus operates at one level above the boot sector but within the heart of the operating system. The virus achieves "stealth" qualities such as hiding its code, making it difficult to trace.

Key
In cryptography, a key is a sequence of symbols that controls the operations of encryption and decryption.

Key logger
A key logger is computer program designed to record which keys are pressed on a computer keyboard. It is used to obtain passwords or encryption leys and thus bypass other security measures.

Kiertsu
Kiertsu is a Japanese term used when supplier and customer organizations have financial interest in each other. It.

Killer packet
A killer packet is a method of disabling a computer system by sending Ethernet or Internet Protocol (IP) packets that exploit bugs in the networking code to crash the system. A similar action is done by synchronized (SYN) floods, which is a method of disabling a computer system by sending more SYN packets than its networking code can handle.

Kiting
Kiting is a scheme in which a depositor with accounts in two or more banks takes advantage of the time required for checks to clear in order to obtain unauthorized credit.

Lapping
Lapping is a type of fraud in which an employee misappropriates receipts from customers and covers the shortages in these customers' accounts with receipts from subsequent customers.

Large power distance culture
A large power distance culture is a culture where a person at a higher position in the organizational hierarchy makes the decisions, and employees at lower levels simply follow the instructions.

Leader
A leader is an individual recognized by others as the person to lead an effort. One cannot be a leader without one or more followers. The term is often used interchangeably with manager. A leader may or may not hold an officially designated management-type position.

Leadership in quality management
Leadership is an essential part of a quality improvement effort. Organization leaders must establish a vision; communicate that vision to those in the organization; and provide the tools, knowledge, and motivation necessary to accomplish the vision.

Leadership grid

A leadership grid is a two-dimensional leadership theory that measures a leader's concern for people and concern for production.

Leading

Leading is: (1) a management function that involves the use of influence to motivate employees to achieve the organization's goals; (2) a strategy used by a firm to accelerate payments, normally in response to exchange rate expectations; the practice of accelerating collections or payments.

Leapfrogging

Leapfrogging is taking a big step forward in thinking up idealistic solutions to a problem. For example, leapfrogging can be applied to value-analyzing comparable products to identify their best features and design. These ideas are then combined into a hybrid product that, in turn, can bring new superior products to enter a new market. It is a problem-solving tool.

Learning organization

A learning organization: (1) is an organization in which everyone is engaged in identifying and solving problems, which enables the organization to continuously experiment, improve, and increase its capability; (2) is an organization that has as a policy to continue to learn and improve its products, services, processes and outcomes; an organization that is continually expanding its capacity to create its future. The term also refers to an organization that accumulates knowledge through the experiences of its employees. Information systems facilitate learning by organizations.

Least privilege

The least privilege principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use.

Legal concepts

Several legal concepts exist as they apply to managers, executives, officers, and board of directors in any organization. For example, officers and directors need to follow duty of due care, duty of loyalty, and duty of obedience, not duty of absolute care or duty of utmost care. Only reasonable and ordinary care is expected of the officers and the board of directors because no one can anticipate all problems or protect from all disasters or losses. Especially, officers and board of directors are expected to follow the highest levels of legal concepts due to their fiduciary and governance responsibilities (i.e., duty of loyalty and duty of obedience). Examples of legal concepts follow:

Due process means following rules and principles so that an individual is treated fairly and uniformly at all times with basic rights protected. It also means fair and equitable treatment to all concerned parties so that no person is deprived of life, liberty, or property without due process of the law, which is the right to notice and a hearing. Due process means each person is given an equal and a fair chance of being represented or heard and that everybody goes through the same process for consideration and approval. It means all people are equal in the eyes of the law. Due law covers due process and due care. Due process requires due care and due diligence.

Two types of due process exist: procedural due process and substantive due process. Procedural due process ensures that a formal proceeding is carried out regularly and in accordance with the established rules and principles. Substantive due process deals with a judicial requirement that enacted laws may not contain provisions that result in the unfair, arbitrary, or unreasonable treatment of an individual. It protects personal property from governmental interference or possession.

Due care means reasonable care in promoting the common good, maintaining the minimal and customary practices, and following the best practices. Due law covers due process and due

care. For example, it is the responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. Another related concept of due care is good faith, which means showing "honesty in fact" and "honesty in intent." Both due care and due diligence are similar to the "prudent man" or "reasonable person" concept.

Due diligence reviews involve pre-assessment, examination, analysis, and reporting on major activities with due care before they are finalized or approved by management. Its purpose is to minimize potential risks from undertaking new businesses and ventures and involving in mergers, acquisitions, and divestitures. Due diligence requires organizations to develop and implement an effective system of controls, policies, and procedures to prevent and detect violation of policies and laws. It requires that the organization has taken minimum and necessary steps in its power and authority to prevent and detect violation of policies and laws. In other words, due diligence is the care that a reasonable person exercises under the circumstances to avoid harm to other persons or to their property. Due diligence is another way of saying due care. Both due care and due diligence are similar to the "prudent man" or "reasonable person" concept. A due diligence defense is available to a defendant in that it makes the defendant not liable if the defendant's actions are reasonable and they are proven.

Due professional care calls for the application of the care and skill expected of a reasonably prudent and competent person in the same or similar circumstances. For example, due professional care is exercised when internal audits are performed in accordance with the IIA Standards. The exercise of due professional care requires that: (1) internal auditors be independent of the activities they audit, (2) internal audits be performed by those persons who collectively possess the necessary knowledge, skills, and disciplines to conduct the audit properly, (3) audit work be planned and supervised, (4) audit reports be objective, clear, concise, constructive, and timely, and (5) internal auditors follow up on reported audit findings to ascertain that appropriate action was taken.

Duty of loyalty is applicable to the officers and the directors of a corporation not to act adversely to the interests of the corporation and not to subordinate their personal interests to those of the corporation and its shareholders.

Duty of care is the legal obligation that each person has to others not to cause any unreasonable harm or risk of harm resulting from careless acts. A breach of the duty of care is negligence. An example is that corporate directors and officers must use due care and due diligence when acting on behalf of a corporation. Duty of reasonable care is same as the duty of care.

Duty of obedience is expected of officers and directors of a corporation to act within the authority conferred upon them by the state corporation statute, the articles of incorporation, the corporate bylaws, and the resolutions adopted by the board of directors.

Legal environment

The legal environment includes rules of competition, packaging laws, patents, trademarks, copyright laws and practices, labor laws, and contract enforcement.

Legitimate power

Legitimate power is power that stems from a formal management position in an organization and the authority granted to it.

Library

A library is a collection of related data files or programs.

Licensing

Licensing: (1) is an arrangement in which a local firm in the host country produces goods in accordance with another firm's (the licensing firm's) specifications; as the goods are sold, the local firm can retain part of the earnings; (2) when a multinational enterprise sells a foreign

company the right to use technology or information. A firm gives a license to another firm to produce or package its product.

Licensing agreement
A licensing agreement is an arrangement in which one firm permits another to use its intellectual property in exchange for compensation, typically a royalty.

Licensing program
In a licensing program, proprietary information, such as patent rights or expertise, are licensed by the owner (licenser) to another party (licensee). Compensation paid to the licenser usually includes license issuance fees, milestone payments, and/or royalties.

Linear cultures
Linear cultures view the past as being behind them and the future in front of them; they view change as good and attempt to take advantage of business opportunities that they foresee.

Linear formula approach
Under the linear formula approach, all rates in the tariff schedules would be reduced across the board by a specific formula, such as certain percentage.

Link-edit
A link-edit is the process of combining object modules to form a load module, which is an executable code for computer processing. It is performed by a linkage editor program.

Link virus
A link virus manipulates the directory structure of the media on which it is stored, pointing the operating system to virus code instead of legitimate code.

Load module
Load module is an IBM term referring to an executable computer program. A program generally begins as a set of statements written in a language such as COBOL or Assembler programming languages. These statements are then translated into machine-specific language called an object module. Although it is in machine language, an object module cannot be executed unless the object code is specifically formatted by a linkage editor to produce a load module. The load module is a complete machine-level program in a form ready to be loaded into main memory and executed.

Local area network (LAN)
A LAN is a data communication network operating over a limited geographical area, typically within a building or group of buildings.

Local content
The term "local content" refers to regulations to gain control over foreign investment by ensuring that a large share of the product is locally produced or a larger share of the profit is retained in the country.

Local content requirements
Local content requirements are the most common form of Trade-Related Investment Measures (TRIMs). They oblige an investor to purchase or use a specific amount of inputs from local suppliers. These requirements are used in an attempt to ensure that the investment increases local employment and develops physical and human capital.

Location decision
A location decision is a decision concerning the number of facilities to establish and where they should be situated.

Locks
Locks are used to prevent concurrent updates to a record. Various types of locks include page level, row level, area, and record.

Locus of control
A locus of control in a person is the tendency to place the primary responsibility for one's success or failure either within oneself (internally) or on outside forces (externally).

Logic bomb
A logic bomb is a resident computer program that triggers an unauthorized or damaging action when a particular event or state in the system's operation is realized (e.g., when a particular packet is received).

Logical record
A logical record is a collection of one or more data item values as viewed by the user.

Lot size
A lot size is the quantity of goods purchased or produced in anticipation of demand.

Low-context culture
A low-context culture is one in which communication is used to exchange facts and information.

Low power distance culture
A low power distance culture is a state in which employees perceive few power differences and follow a superior's instructions only when either they agree or feel threatened.

Machiavellianism
Machiavellianism is the tendency to direct much of one's behavior toward the acquisition of power and the manipulation of others for personal gain.

Machine cycle
A machine cycle is the basic operating cycle of a computer processor during which a single program instruction is fetched, interpreted, and executed. Same as central processing unit cycle, execution cycle.

Machine productivity
Machine productivity is a partial productivity measure. It is the rate of output of a machine per unit of time compared with an established standard or rate of output. Machine productivity can be expressed as output per unit of time or output per machine-hour.

Machine utilization
Machine utilization is a measure of how intensively a machine is being used. It compares the actual machine time (setup and run time) to available time.

Macroassessment
Macroassessment is the overall risk assessment of a country without considering the multinational enterprise's business.

Macroeconomic level
The macroeconomic level is the level at which trading relationships affect individual markets.

Macro virus
A specific type of computer virus that is encoded as a macro embedded in some document and activated when the document is handled. It is a virus that attaches itself to application documents, such as word processing files and spreadsheets, and uses that application's macro-programming language to execute and propagate.

Mailbombing
Mailbombing means flooding a site with enough mail to overwhelm its e-mail system. It is used to hide or prevent receipt of e-mail during an attack or as a retaliation against a site.

Main memory
Main memory is memory that can be directly accessed by the processor.

Malware
Malware is malicious software or malicious code that contains computer instructions intended for abnormal program behavior. Contrast this behavior to unexpected program behavior due to errors or bugs introduced accidentally. Malware is designed to deny, destroy, modify, or impede the software's logic, configuration settings, data, or program library routines. It can be inserted during software development, preparation for distribution, deployment, installation, and/or update. It can be planted manually or through automated means, and it can also be inserted during a system's operation. Regardless of when in the software life cycle the malware is embedded, it effectively becomes part of the software and can present substantial dangers and risks.
There are several ways in which malware is likely to be inserted during software development or maintenance through a back door or trapdoor, time bomb, logic bomb, and software holes. Malware is introduced into a system due to unnoticed, forgotten, or neglected functions or when unnecessary functions are disregarded. It can be discovered through table-top reviews, periodic assessments, war dialing, war driving, wireless scanning, and penetration testing. Examples of malware planted on operational systems include viruses, worms, Easter eggs, Trojan horses, zombies, cross-site scripts, botnets, rootkits, cookies, adware, spyware, vandalware, active content (Active X), applets, application program interface (API), electronic Dumpster diving, and buffer overflow.

Management science
Management science or operations research provides management an approach that focuses on decision making and reliance on formal mathematical models. It is a decision-making tool.

Manager
A manager is an individual who manages and is responsible for resources (people, material, money, time). A person officially designated with a management-type position title. A manager is granted authority from above, whereas a leader derives his or her role by virtue of having followers. However, the terms "manager" and "leader" are often used interchangeably.

Managerial grid
A managerial grid is part of a management theory developed by Robert Blake and Jane Mouton that maintains that a manager's management style is based on his or her mind-set toward people; it focuses on attitudes rather than behavior. The grid is used to measure concern with production and concern with people.

Mandatory access control (MAC) policy
MAC policy is driven by the results of a comparison between the user's trust level/clearance and the sensitivity designation of the information. MAC is a means of restricting access to objects (system resources) based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects (users) to access information of such sensitivity. *Compare* with Discretionary access control (DAC) policy.

Manifest
A manifest is an itemization of the items shipped; a copy of the freight bill.

Map
A map is a software measurement tool that analyzes a computer program during processing a current indicate which program statements have been executed

Market grade
If a product is market grade, it is of fair, average quality. The grade is used in applying the implied warranty of merchantability.

Markov chain
The Markov chain is a decision-making tool to determine outcomes in which the outcome of an event is dependent on the outcome of previous events.

Margin of dumping
The margin of dumping is the percent by which the price charged for the same or a like product in the home market of the exporter exceeds the export price.

Market entry strategy
A market entry strategy is an organizational strategy for entering a foreign market.

Masculinity in culture
Masculinity: (1) is a cultural preference for achievement, heroism, assertiveness, work centrality, and material success; (2) is the relative importance of the qualities associated with men, such as assertiveness and materialism; (3) refers to the degree to which people in a society stress material success and assertiveness and assign different roles to males and females.

Masculinity/femininity in culture
Masculinity/feminity are dimensions of cultures that refer to the degree to which "masculine" values prevail over "feminine" values.

Mask works
Mask works are the patterns on the surface of a semiconductor chip.

Maslow's Hierarchy of Needs
Maslow's Hierarchy of Needs is a classification scheme of needs satisfaction where higher-level needs are dormant until lower-level needs are satisfied.

Masquerading
Several definitions exist for masquerading: (1) impersonating an authorized user and gaining unauthorized privileges; (2) an unauthorized agent claiming the identity of another agent; (3) an attempt to gain access to a computer system by posing as an authorized user; and (4) the pretense by which an entity pretends to be a different entity. It is synonymous with impersonating, mimicking, and spoofing.

Material injury
Under the Tariff Act of 1930, as amended, the term "material injury" means "harm which is not inconsequential, immaterial, or unimportant." In determining material injury, the International Trade Commission considers domestic consumption, U.S. production, capacity, capacity utilization, shipments, inventories, employment, and profitability.

Matrix approach
The matrix approach is an organization structure that utilizes functional and divisional chains of command simultaneously in the same part of the organization.

Matrix organization
A matrix organization is an organization in which managers report to both a divisional executive and a functional executive. For instance, the marketing manager of the

manufacturing division reports both to the division's president and to the corporate vice president of marketing.

Matrix organization structure

The matrix organization structure is a hybrid of the functional and project organizational structures, in which resources from appropriate functional components of a company are temporarily assigned to particular projects.

Matrix structure

The term "matrix structure": (1) describes an organization that is organized into a combination of functional and product departments; it brings together teams of people to work on projects and is driven by product scope; (2) refers to an organizational structure that uses functional and divisional structures simultaneously. This structure is strongly decentralized: It allows local subsidiaries to develop products that fit into local markets. Yet, at its core, it is very centralized: It allows companies to coordinate activities across the globe and capitalize on synergies and economies of scale.

Mean time between failures (MTBF)

Mean time between failures (MTBF) is the average length of time a system is functional or the average time interval between failures. It is total functioning life of an item divided by the total number of failures during the measurement interval of minutes, hours, and days. It is the average length of time a system or a component works without fault between consecutive failures. MTBF assumes that the failed system is immediately repaired as in MTTR. A high MTBF means high system reliability. MTBF = MTTF + MTTR.

Mean time between outages

Mean time between outages (MTBO) is the mean-time between equipment failures that result in a loss of system continuity or unacceptable degradation, as expressed by MTBO = MTBF/(1-FFAS), where MTBF is the non-redundant mean-time between failures and FFAS is the fraction of failures for which the failed hardware or software is bypassed automatically. A low MTBO means high system availability.

Mean time to data loss

Mean time to data loss (MTTDL) is the average time before a loss of data occurs in a given disk array and is applicable to redundant array of independent disk (RAID) technology. A low MTTDL means high data reliability.

Mean time to failure

Mean time to failure (MTTF) is the average time to the next failure. It is the time taken for a part or system to fail for the first time. MTTF assumes that the failed system is not repaired. A high MTTF means high system reliability.

Mean time to repair (MTTR)

Mean time to repair (MTTR) is the amount of time it takes to resume normal operation. It is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time. A low MTTR means high system reliability.

Memory card

A memory card is a removable data storage device used for personal authentication, access authorization, card integrity, and application systems. A memory card is made up of nonvolatile flash memory chips.

Metropolitan area network (MAN)

MAN is a network concept aimed at consolidating business operations and computers spread out in a town or city.

Migration
Migration is a term generally referring to the moving of data from an online storage device to an offline or low-priority storage device, as determined by the system or as requested by the system user.

Mirrored sites
Mirrored sites are fully redundant facilities with automated real-time information mirroring. A mirrored site (redundant site) is equipped and configured exactly like the primary site in all technical respects. Some organizations plan on having partial redundancy for disaster recovery purposes and partial processing for normal operations. The stocking of spare personal computers and their parts or local area network servers also provide some redundancy. Mirrored sites are a part of information technology continuity planning.

Mobile sites
Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. Mobile sites are a part of information technology continuity planning.

Modem
Acronym for modulation/demodulation. During data transmission, the modem converts the computer representation of data into an audio signal for transmission on telephone, teletype, or intercom lines. When receiving data, the modem converts the audio signal to the computer data representation.

Modular design
Modular design is information system project design that breaks the development of a project into various pieces (modules) that each solve a specific part of the overall problem. These modules should be as narrow in scope and brief in duration as practicable. Such design minimizes the risk to an organization by delivering a net benefit that is separate from the development of other pieces.

Monoculture
A monoculture is a culture that accepts only one way of doing things and one set of values and beliefs.

Morphological analysis
Morphological analysis is a system involving the methodical interrelating of all elements of a problem in order to discover new approaches to a solution. It is a problem-solving tool.

Most-favored nation (MFN)
A term describing a General Agreement on Tariffs and Trade/World Trade Organization clause that calls for member countries to grant other member countries the same most favorable treatment they accord any country concerning imports and exports.

Most-favored-nation (MFN) treatment
MFN treatment is a principle of nondiscrimination that commits all General Agreement on Tariffs and Trade or World Trade Organization signatories to extend the same treatment to all other signatories.

Multidomestic approach
The multidomestic approach is an approach to international marketing in which the firm adapts to local conditions in each and every target market.

Multidomestic strategy
Multidomestic strategy (1) refers to the modification of product design and advertising strategies to suit the specific needs of individual countries; (2) is a business strategy where each individual country organization is operated as a profit center.

Multilateral negotiations
Multilateral negotiations are trade negotiations among more than two parties; the intricate relationships among trading countries.

Multinational corporation (MNC)
An MNC is a company that: (1) receives more than 25% of its total sales revenues from operations outside the parent company's home country; also called global corporation or transnational corporation; (2) has production operations in at least one country in addition to its domestic base; (3) considers the globe as a single marketplace; (4) invests in countries around the globe. MNCs are international businesses that establish subsidiaries in foreign markets.

Multinational enterprise (MNE)
An MNE is: (1) any business that engages in transactions involving the movement of goods, information, money, people, or services across national borders; (2) an organization with operating units located in foreign countries. Also called multinational corporation.

Multinational restructuring
Multinational restructuring is restructuring of the composition of an multinational corporation's assets or liabilities.

Multipartite virus
A multipartite virus is a combination of both boot sector and file infector viruses, which can be spread by both methods.

Multiple Virtual Storage (MVS)
MVS is an IBM virtual storage operating system that gives each user a processing environment that is defined as an address space. It provides for the isolation and protection of one user from another in a multiprogramming system supporting many users concurrently.

Multiplexor
A multiplexor is a device used to combine the data being transmitted over a number of low-bandwidth data links for transmission over one or more channels of higher bandwidth and vice versa.

Multiprocessor
A multiprocessor is a computer that consists of several processors which may execute programs simultaneously.

Multiprogramming
Same as *multitasking*.

Multitasking
The concurrent execution of several programs. Same as *multiprogramming*.

Multithreading
Multithreading is code in a program designed to be available for servicing multiple tasks at once, in particular by overlapping input/output.

Nationalization
Nationalization occurs when a government takes over private property. The government usually pays reasonable compensation.

Natural hedges
Natural hedges are created from the relationship between revenues and costs of a business unit or a subsidiary. The more revenues over the cost, the better the protection is. The key is the extent

to which cash flows adjust naturally to currency changes due to exchange-rate fluctuations. One way to explore the likelihood of a natural hedge is to determine whether a subsidiary's revenue and cost functions are sensitive to domestic or global business conditions.

Many types of risks may be relatively correlated with each other. Consequently, combining these risks produces a form of natural hedging. The traditional silo approach could actually reduce the overall efficiency of the firm's risk management activities by destroying the natural hedging that exists at the enterprise-wide level.

Natural team

A natural team is a work group having responsibility for a particular process.

Needs

The term "needs" refers to unsatisfactory conditions of the consumer that prompt him or her to an action that will make the condition better.

Negotiation

Negotiation is a process of formal communication, either face to face or electronic, where two or more people come together to seek mutual agreement about an issue or issues.

Net foreign direct investment

Net foreign direct investment is the value of any new foreign direct investment that enters a country in one year minus any reduction in foreign direct investment in that country in that year.

Network

A network consists of two or more computers linked by communication lines.

Node

A node is a communication point at which subordinate items of data originate. Examples include cluster controllers, terminals, computers, networks.

Nominal group technique

The nominal group technique is an idea-generating, consensus-building tool for problem-solving. No real group exists; it is a group in name only. A strength of this technique is that it permits a problem to become focused in a short period of time.

Nonactionable subsidies

Nonactionable subsidies are permissible subsidies, against which General Agreement on Tariffs and Trade or World Trade Organization remedies cannot be sought as long as they are structured according to certain criteria.

Nontariff barriers

Nontariff barriers include quotas, bans, safety standards, and subsidies. Sometimes they are employed by governments to restrict trade or reduce competition. Nontariff barriers occur when governments impose restrictive and costly administrative and legal requirements on imports.

Nontariff trade barriers

The General Agreement on Tariffs and Trade and later World Trade Organization has developed many categories of nontariff trade barriers. Most of them are measures used at the border to restrict the inflow of foreign goods. Major categories of nontariff trade barriers include quantitative import restrictions, such as quotas, voluntary export restraints, and price controls.

Norming

Norming is the stage of team development in which conflicts developed during the storming stage are resolved and team harmony and unity emerge.

Norms
Norms are behavioral expectations, mutually agreed-on rules of conduct, protocols to be followed, and social practice.

Object
An object is a passive entity that contains or receives information. Examples of objects are records, blocks, files, and programs.

Object-based virus
Major office application programs are written in objects, so they can be reused. These objects are loaded into random access memory and linked together only when they are needed. An object-based virus infects the object and avoids normal methods of detection. Most antivirus software packages protect and monitor executable files, not objects.

Object code/module
An object code/module is source code compiled to convert to object code, a machine-level language or computer software.

Objective risk
Objective risk differs from subjective risk primarily in the sense that it is more precisely observable and therefore measurable. In general, objective risk is the probable variation of actual from expected experience.

Offline storage
Offline storage refers to the storage of data on media that are physically removed from the computer system and stored elsewhere (e.g., a magnetic tape or a floppy disk).

Offsets
Offsets are various concessions sometimes required by a purchaser. They include requiring bidders to provide: (1) local content in goods, (2) technology transfer to the purchaser, (3) some investment in the country, or (4) trade in other areas.

Offsite storage
In offsite storage, backup programs, data files, forms, and documentation, including a contingency plan, are stored in a location remote from the primary computer facility. These are used at backup computer facilities during a disaster or major interruption at the primary computer facility.

Open-end order
An open-end order is an order specifying all terms except quantity; it is similar to a blanket order.

Operating system (OS)
An OS is an integrated collection of computer programs, service routines, and supervising procedures to operate a computer (i.e., scheduling of jobs, loading of programs, allocation of memory, file management, controlling of input/output operations).

Operating system (OS) (console) log
An OS log provides information on who used computer resources, for how long, and for what purpose. Unauthorized actions can be detected by analyzing the OS log.

Operational goals
Operational goals are specific, measurable results expected from departments, work groups, and individuals within the organization.

Operational managers
Operational managers are individuals who are in charge of small groups of workers.

Operational plans
Operational plans are plans developed at the organization's lower levels that specify action steps toward achieving operational goals and that support tactical planning activities.

Operational risk
Operational risk is a risk related to the organization's internal systems, products, services, processes, technology, and people.

Operations
Operations: (1) is the collection of people, technology, and systems within a company that has primary responsibility for providing the organization's products or services; (2) used with "objectives" or "controls," has to do with the effectiveness and efficiency of an entity's operations, including performance and profitability goals and safeguarding resources.

Operations research
Operations research is a management science discipline attempting to find optimal solutions to business problems using mathematical techniques, such as simulation, linear programming, statistics, and computers. It is a problem-solving tool.

Operations strategy
Operations strategy is the recognition of the importance of operations to the firm's success and the involvement of operations managers in the organization's strategic planning.

Optical fiber
Optical fiber is a thin filament of glass or other transparent material through which a signal-encoded light beam may be transmitted by means of total internal reflection.

Option
An option is a contract that provides the right to buy or sell a given amount of currency at a fixed exchange rate on or before the maturity date. It is a financial market.

Organic organization
An organic organization allows employees considerable discretion in defining their roles and the organization's objectives. Historically, small organizations have tended to adopt the organic form.

Organisation for Economic Co-operation and Development (OECD)
The OECD promotes worldwide economic development in general and economic growth and stability of its member countries in particular. Its work focuses primarily on providing financial accounting and reporting guidelines to multinational corporations for disclosures to host countries.

Organization
An organization is a social entity that is goal directed and deliberately structured.

Organizational behavior
Organizational behavior is an interdisciplinary field dedicated to the study of how individuals and groups tend to act in organizations.

Organizational change
Organizational change refers to the adoption of a new idea or behavior by an organization.

Organizational control
Organizational control is the systematic process through which managers regulate organizational activities to make them consistent with expectations established in plans, targets, and standards of performance.

Organizational culture
Organizational culture is: (1) the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration; having worked well enough to be considered valid, the pattern may be taught to new members as the correct way to perceive, think, and feel in relation to those problems; (2) an umbrella term referring to the general tone of a corporate environment.

Organizational development
Organizational development is the application of behavioral science techniques to improve an organization's health and effectiveness through its ability to cope with environmental changes, improve internal relationships, and increase problem-solving capabilities. It organization-wide (usually) planned effort, managed from the top, to increase organization effectiveness and health through interventions in the organization's processes, using behavioral science knowledge.

Organization structure
Organization structure is the framework in which the organization defines how tasks are divided, resources are deployed, and departments are coordinated.

Overhead
Overhead is the amount of processing resources required to perform system functions as compared to those necessary to perform the application transaction.

Overlay
Overlay refers to storing a program module in the main memory space previously allocated to another, no-longer-needed module of the same program.

Overwriting virus
An overwriting virus destroys code or data in the host program by replacing it with the virus code. Most viruses attempt to retain the original host program's code and functionality after infection because the virus is more likely to be detected and deleted if the program ceases to work. A nonoverwriting virus is designed to append the virus code to the physical end of the program or to move the original code to another location.

Ownership risk
Ownership risk is the risk inherent in maintaining ownership of property abroad. It is the exposure of foreign-owned assets to government intervention.

P > O expectancy
P > O expectancy is the expectancy that successful performance (P) of a task will lead to the desired outcome (O).

Padded cell systems
Padded cell systems take a different approach from honeypots and honey nets. Instead of trying to attract attackers with tempting data, a padded cell waits for traditional intrusion detection and prevention systems to detect an attacker. The attacker is then seamlessly transferred to a special padded cell host. The attacker may not realize anything has happened but is now in a simulated environment where it can not cause any harm caused. Like the honeypot, this simulated environment can be filled with interesting data to convince an attacker that the attack is going according to plan. Padded cells offer unique opportunities to monitor the actions of an attacker. Padded cell systems complement intrusion detection systems.

Page
A page is a fixed-length independently addressed portion of a program that can be loaded into noncontiguous memory.

Paging
Paging is the process of: (1) dividing a program into fixed-length pages and (2) swapping pages between the real page pool and the external paging device.

Panel consensus technique
The panel consensus technique is a way to process a large number of ideas, circumventing organizational restraints to idea creation, using extensive participation and emphasizing methods for selecting good ideas. It is a problem-solving tool.

Parasitic virus
Parasitic viruses are more numerous but less prevalent than boot sector viruses. They are considered file infectors because they infect executable files.

Parity bit
A parity bit is a bit indicating whether the sum of a previous series of bits is even or odd.

Parent company
A parent company is the company owning a majority of the voting stock of another corporation.

Parent/subsidiary relationship
A parent/subsidiary relationship is combination of companies where control of other companies, known as subsidiaries, is achieved by a company, known as the parent, through acquisition of voting stock.

Pareto chart
A Pareto chart can be drawn to separate the "vital few" from the "trivial many." It is based on the 80/20 rule: 20% of items contribute to 80% of problems. It is a problem-solving tool.

Participative management
Participative management is a management style that expects everyone in the organization to take ownership and responsibility for their conduct and responsibilities and that allows input into decisions.

Parity checking
Parity checking is a hardware control in computers that detects data errors during transmission. It compares the sum of a previous set of bits with the parity bit to determine if an error in the transmission or receiving of the message has occurred.

Partnership/alliance
A partnership/alliance is a strategy leading to a relationship with suppliers or customers aimed at reducing costs of ownership, maintenance of minimum stocks, just-in-time deliveries, joint participation in design, exchange of information on materials and technologies, new production methods, quality improvement strategies, and the exploitation of market synergy.

Passive investment strategy
A passive investment strategy involves a minimal amount of oversight and very few transactions once the portfolio has been selected.

Passphrase
A passphrase is a unique password, not like a simple password, and is both strong and easy to remember. It follows several safeguard guidelines: It is longer than simple, or normal password, it is not a common phrase, and it includes numbers, both lowercase and uppercase letters, and special characters (e.g., dollar sign, pound sign, or punctuation).

Patch management
Patch management is the process of acquiring, testing, and distributing patches, fixes, and service packs to the appropriate system administrators and users throughout the organizations.

Patent
A patent protects an invention by giving the inventor the right to exclude others from making, using, or selling a new, useful, nonobvious invention during a specific patent term.

Path-goal theory
Path-goal theory is a contingency approach to leadership specifying that the leader's responsibility is to increase subordinates' motivation by clarifying the behaviors necessary for task accomplishment and rewards.

Pay compression
Pay compression is a situation in which pay differences among individuals with different levels of experience and performance in the organization becomes small.

Pay equity
Pay equity is the similarity in pay for all jobs requiring comparable levels of knowledge, skill, and ability, even if actual duties and market rates differ significantly.

Pay for performance
Pay for performance refers to incentive pay that ties at least part of compensation to employee effort and performance.

Payoff table
A payoff table is a tabular representation of the payoffs for a decision problem. It shows losses and gains for each outcome of the decision alternatives. It is a decision-making tool.

Peer review
Peer review is a quality assurance method in which two or more programmers review and critique each other's work for accuracy and consistency with other parts of the system. It is a detective control.

Peer to peer (P2P)
P2P is an Internet network in which a group of computer users, each equipped with the same networking program, can connect to each other and directly access files from one another's computers. Use of P2P can be risky due to data sharing and malware spreading.

Penetration testing
Penetration testing is laboratory-based testing. It consists of: (1) pretest analysis based on full knowledge of the target system, (2) pretest identification of potential vulnerabilities based on pretest analysis, and (3) current testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed on by all parties before the commencement of any penetration testing scenario.

Perfective maintenance
The term "perfective maintenance" to all changes, insertions, deletions, modifications, extensions, and enhancements made to a system to meet the user's evolving or expanding needs.

Performance
Performance is: (1) the organization's ability to attain its goals by using resources in an efficient and effective manner; (2) what an employee does or does not do.

Performance appraisal
A performance appraisal is the process of evaluating how well employees perform their jobs when compared to a set of standards and then communicating that information to employees.

Performance-based pay
Performance-based pay is pay related to and directly derived from performance.

Performance consulting
Performance consulting is a process in which a trainer and the organizational client work together to boost workplace performance in support of business goals.

Performance gap
A performance gap is a disparity between existing and desired performance levels.

Performance management system
A performance management system is: (1) a system that supports and contributes to the creation of high-performance work and work systems by translating behavioral principles into procedures; (2) processes used to identify, encourage, measure, evaluate, improve, and reward employee performance.

Performance measurement
Performance measurement is the process of developing measurable indicators that can be systematically tracked to assess progress made in achieving predetermined goals and using such indicators to assess progress in achieving these goals.

Performance plan
A performance plan is a performance management tool that describes desired performance and provides a way to assess the performance objectively.

Performance report
A performance report is a routine report that compares actual performance against budgetary goals.

Performance shares
Performance shares are used in incentive plans in which managers are awarded shares of stock on the basis of the firm's performance with respect to earnings per share or other measures.

Performance standards
Performance standards are expected levels of performance.

Performance test
A performance test is an assessment device that requires candidates to complete an actual work task in a controlled situation.

Performing
Performing is the stage of team development in which members focus on problem solving and accomplishing the team's assigned task.

Peril
Peril is the cause of possible loss, the event insured against. "Open peril" is a term used to describe a broad form of property insurance in which coverage applies to loss arising from any fortuitous cause other than those perils or causes specifically excluded.

Periodic review system
A periodic review system is a fixed-order interval inventory control system in which an item's inventory position is reviewed on a scheduled periodic basis.

Perpetual inventory system
A perpetual inventory system maintains information about both receipts and withdrawals for each item in the inventory. The system shows the current balance on hand, which can be reconciled to the actual physical inventory on the floor.

Pharming attack
A pharming attack is a computer attack in which an attacker corrupts an infrastructure service, such as the domain name system (DNS) causing the subscriber to be misdirected to a forged

verifier/relying party and to reveal sensitive information, download harmful software, or contribute to a fraudulent act. It uses DNS server software to redirect users into accessing a fake Web site masquerading as a legitimate one and divulging personal information. It is a digital form of social engineering technique.

Phishing attack
A phishing attack is a compter attack in which the subscriber is lured (usually through an e-mail) to interact with a counterfeit verifier and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier. It is a digital form of social engineering technique that uses authentic-looking but phony (bogus) e-mails to request personal information from users or direct them to a fake Web site that requests such information. It tricks or deceives individuals into disclosing sensitive personal information through deceptive computer-based means.

Physical record
A physical record is a unit of data accessed by the hardware from some storage medium (e.g., disk).

Piggyback entry
Piggyback entry is unauthorized access that is gained to an information system facility or system via another user's legitimate connection.

Platform
A platform is the foundation technology (bottommost layer) of a computer system. The term also refers to the type of computer (hardware) or operating system (software) being used.

Plan-do-check-act cycle (PDCA)
The PDCA cycle, which consists of four phases, is a core management tool for problem solving and quality improvement. The "plan" phase calls for developing an implementation plan for initial effort followed by organization-wide effort. The "do" phase carries out the plan on a small-scale using a pilot organization and later on a large-scale. The "check" phase evaluates lessons learned by the pilot organization. The "act" phase uses the lessons learned to improve the implementation.

Plug-ins
Plug-ins are computer applications intended for use in the Web browser (e.g., Adobe Flash). Plug-ins are similar to Microsoft's Active X controls but cannot be executed outside of a Web browser. Plug-ins can be risky because they can contain programming flaws, such as buffer overflows, or they may contain design flaws, such as cross-domain violations.

Pluralism of organizations
The term "pluralism" refers to the state of an organization that accommodates several subcultures, including employees who would otherwise feel isolated and ignored.

Plurilateral agreements
Plurilateral agreements are those Uruguay Round agreements not signed by all World Trade Organization members. These include the Agreement on Trade in Civil Aircraft, the Agreement on Government Procurement, the International Dairy Arrangement, and the Arrangement Regarding Bovine Meat.

PM theory of leadership
The PM theory of leadership is a Japanese theory; the "P" stands for showing a concern for subordinates and leadership that is oriented toward forming and reaching group goals; the "M" stands for leadership that is oriented toward preserving group stability.

Pointer
A pointer is an address stored in memory that provides a link to a related data field, data file, record, and control block.

Political risk
Political risk: (1) is the risk of loss by an international corporation of assets, earning power, or managerial control as a result of political actions by the host country; (2) a political action taken by the host government or the public that affect the multinational corporation's cash flows. It is the risk of expropriation (seizure) of a foreign subsidiary's assets by the host country or of unanticipated restrictions on cash flows to the parent company.

Poka-yoke
Poka-yoke is a mistake-proofing, fail-safe work method, or fail-safe technique by which errors are prevented from resulting in a product defect. It is a Japanese term.

Polling
Polling is an alternative to contention. It makes sure that no terminal is kept waiting for a long time.

Polycentric staffing outlook
The polycentric staffing outlook is the belief that key positions in foreign subsidiaries should be staffed by host-country nationals (locals).

Polymorphic virus
During replication, a polymorphic virus creates instructions that are functionally equivalent but have distinctly different byte streams. To achieve this, the virus may randomly insert superfluous instructions, change the order of independent instructions, or choose from a number of different encryption schemes. This variable quality makes the virus difficult to locate, identify, or remove. A polymorphic virus produces varied copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus. These copies are operational in nature. A simple boot sector or file virus is transformed into a polymorphic virus using a mutation engine, which further proliferates. Polymorphic viruses are difficult to detect due to their proliferation.

Port
A port is an interface mechanism (e.g., a connector, a pin, or a cable) between a peripheral device (e.g., printer, terminal) and the central processing unit.

Portability
The term "portability" describes the ease with which software can be transferred from one computer system to another.

Portfolio approach
The portfolio approach is a method used to manage economic exposure of a company by offsetting negative exposure in one country with positive exposure in another.

Portfolio risk
Portfolio risk considers risk and return of a firm when it is investing in acquisition or expansion projects. Management needs to find the relationship between the net present values (NPVs) for new projects and the NPVs for existing projects. In a portfolio framework, the trade-off between risk and expected NPV for different combinations of investments can be analyzed.

Portfolio strategy
Portfolio strategy is a type of corporate-level strategy that pertains to the organization's mix of strategic business units and product lines that fit together in such a way as to provide the corporation with synergy and competitive advantage.

Power
Power refers to the potential ability to influence others' behavior.

Power distance
Power distance: (1) is the degree to which people accept inequality in power among institutions, organizations, and people; (2) a dimension of culture that refers to the inequality among the people of a nation; (3) refers to the degree to which people in a society accept centralized power and depend on superiors for structure and direction.

Predatory dumping practices
Predatory dumping practices involve large and economically powerful firms using market leverage to drive small firms out of business, thus reducing competition so the predatory larger firms can then raise prices and reap monopoly profits.

Pre-expatriation program
Once the expatriate has been selected for the foreign assignment, but before leaving the home country, he or she is involved in a pre-expatriation program, which involves training to prepare for what will be encountered in the foreign country.

Pretty good privacy (PGP)
PGP is a computer program used to encrypt and decrypt data, primarily e-mail, over the Internet.

Prevention costs
Prevention costs are associated with all the activities that focus on preventing defects. It is the cost of conformance to quality standards. Some major cost categories included in this cost classification are: operator inspection costs, supplier ratings, supplier reviews, purchase order technical data reviews, training, supplier certification, design reviews, pilot projects, prototype test, vendor surveys, quality design, and quality department review costs. These costs are associated with poor quality of products or services if defects are not prevented.

Preventive maintenance
With preventive maintenance, computer hardware and related equipment are maintained on a planned basis by the manufacturer, vendor, or third party to keep them in a continued operational condition.

Price-averaging calculations
Price-averaging calculations are used in antidumping cases to compare the exporting country's home market price for the subject merchandise to the export price for the same merchandise. This comparison may be based on (1) the weighted average of the home market prices to the weighted average of the export prices; and (2) individual to weighted average prices, in cases where it can be shown that spot dumping is occurring or where data are not available. In addition, individual home market prices may be compared to individual export prices.

Primary product
A primary product is a farm, forest, or fishery product.

Prisoner's dilemma
The prisoner's dilemma is a type of business game situation where one firm is concerned about the actions of its rivals. It is a decision-making tool.

Privileged instruction
A privileged instruction is an instruction that can be executed only by an operating system routine.

Problem state
A problem state is a state in which a computer is executing an application program.

Process
A process is a set of interrelated resources and activities that transform inputs into outputs.

Process owner
A process owner is an individual held accountable and responsible for the workings and improvement of one of the organization's defined processes and its related subprocesses.

Process theories
Process theories explain how employees select behaviors with which to meet their needs and determine whether their choices were successful.

Processed material
A processed material is a tangible product generated by transforming raw material into a desired state. This state can be liquid, gas, particulate, material, ingot, filament, or sheet.

Product
A product is the result of activities or processes.

Product cycle theory
Product cycle theory : (1) suggests that a firm initially establish itself locally and expand into foreign markets in response to foreign demand for its product; over time, the multinational corporation will grow in foreign markets; after some point, its foreign business may decline unless it can differentiate its product from competitors; (2) views products as passing through four stages: introduction, growth, maturity, decline. During these stages, the location of production moves from industrialized to lower-cost developing nations.

Product differentiation
Product differentiation is the effort to build unique differences or improvements into products.

Product division structure
Each of the enterprise's product divisions is responsible for the sale and profits of its product.

Productive capacity
Productive capacity is the maximum of the output capabilities of a resource or the market demand for that output for a given time period.

Product life cycle
A product life cycle is a cycle of stages that a product goes through from birth to death: introduction, growth, maturity, and decline.

Product organization
In a product organization, each department focuses on a specific product type or family.

Product/service strategy
Managers are typically concerned with what the product or service should look like and what it should be able to do. In foreign markets, they must determine whether their product or service can be sold in standard form or be customized to fit differing foreign market needs.

Program interrupt
A program interrupt is an interrupt that results from an illegal or invalid instruction.

Program optimizer
A computer program optimizer removes inefficient or dead code in source programs, which in turn, allows to generate efficient object code from the source code.

Program properties table (PPT)
A PPT is a table that contains names of special programs with their codes and properties.

Progress payments
Progress payments are payments specified in a contract to be made at specific times, based on a supplier's progress in completing the job.

Prospective pricing
Prospective pricing is a pricing decision made in advance of performance, based on an analysis of comparative prices, cost estimates, past costs, or combinations of such considerations.

Protective capacity
Protective capacity is the amount of extra capacity at nonconstraints above the system constraint's capacity, used to protect against statistical fluctuations (e.g., equipment breakdowns, quality problems, late deliveries).

Protocol
A protocol is a set of rules that govern the way in which computers or other functional units transfer data.

Prototyping
Prototyping is a hardware and software development technique in which a preliminary version of part or all of the hardware or software is developed to permit user feedback, determine feasibility, or investigate timing or other issues in support of the development process.

Psychodramatic approach
The psychodramatic approach is a problem-solving tool that involves role-playing and role-reversal behavior. In psychodrama, the attempt is made to bring into focus all elements of an individual's problem; here, as in sociodrama, the emphasis is on shared problems of group members.

Pure risk
Risk is a possibility of loss. Many types of risks exist, including pure risk, speculative risk, static risk, dynamic risk, subjective risk, and objective risk. Pure risk is a condition in which there is the possibility of loss or no loss (e.g., default of a debtor or disability). Pure risks are of several types, including personal, property, liability, and performance risks. Risk management is a scientific approach to the problem of dealing with the pure risks facing an individual or an organization. Insurance is viewed as simply one of several approaches for dealing with such risks. The techniques of insurance and self-insurance are commonly limited to the treatment of pure risks, such as fire, product liability, and worker's compensation. Traditionally, risk management tools—avoidance, loss control, and transfer—have been applied primarily to the pure or hazard risks facing a firm.

Purging
Purging is the removal of sensitive data from storage media at the end of a period of processing, including from peripheral devices with storage capacity, in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed through open-ended laboratory techniques (i.e., information scavenging through laboratory equipment). The storage media must be disconnected from any external network before a purge. A potential risk is reconstruction of data if the purging operation is not performed properly.

Put option
A put option is an option to sell currency. It is a financial market.

Quad
During the Uruguay Round, the Quad consisted of the United States, Japan, the European Union, and Canada to promote international trade.

Quality

Quality is the totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs. It refers to "fitness for use" or "fitness for purpose."

Quality assurance

Quality assurance (QA) is a program by which the director of internal auditing evaluates the operations of the internal auditing department. The purpose of the quality assurance program is to provide reasonable assurance that internal auditing work conforms to the IIA *Standards*, the internal auditing department's charter, and other applicable standards. The quality assurance program should include these elements: (1) supervision, (2) internal reviews, and (3) external reviews. Quality assurance in information systems

QA is an information technology program by which an independent information system (IS) staff reporting to the highest IS executive, provides assurance to management that proper standards and procedures for systems planning, design, development, implementation, operation, and maintenance are followed to produce a quality computer system that satisfies functional user requirements.

Quality audit

A quality audit is a systematic and independent examination to determine whether quality activities comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives.

Quality control

Quality control is the operational techniques and activities that are used to fulfill requirements for quality.

Quality control charts

All quality control charts use statistics and include control charts, run charts, and cusum charts. They are used mainly in manufacturing to limit process variation and to improve process stability.

A *control chart* assesses a process variation and displays sequential process measurements relative to the overall process average and control limits. The upper and lower control limits establish the boundaries of normal variation for the process being measured. Variation within control limits is attributable to random or chance causes, while variation beyond control limits indicates a process change due to causes other than chance—a condition that may require investigation. The upper control limit and lower control limit give the boundaries within which observed fluctuations are typical and acceptable. These limits usually are set, respectively, at 3 standard deviations above and below the mean of all observations.

There are many different types of control charts, including: np, the number of nonconforming units; p, a fraction of nonconforming units; c, the number of nonconformities; u, the number of nonconformities per unit; X, a single observed value; XB, X-Bar; R, a range; XM, a median; and MR, a moving range. The *range chart* (R chart) measures the variability within a manufacturing process, which is expressed as a range of values.

A *run chart* is a simplified control chart, in which the upper and lower control limits are omitted. The purpose of the run chart is more to determine trends in a process rather than its variation. Run charts can be used effectively to monitor a process, for example, to detect sudden changes and to assess the effects of corrective actions. Run charts provide the input for establishing control charts after a process has matured or stabilized in time. Limitations of this technique are that it analyzes only one characteristic over time, and it does not indicate if a single data point is an outlier. *Cusum charts* require that dimensions of a product that are of interest can be measured easily.

Quality management
Quality management refers to all activities of the overall management function that determine the quality policy, objectives, and responsibilities, and implement them by means such as quality planning, quality control, quality assurance, and quality improvement within the quality system. It is achieving results that satisfy the user requirements for quality.

Quality manual
A quality manual is a document stating the quality policy and describing the quality system of an organization.

Quality plan
A quality plan is a document describing specific quality practices, resources, and sequence of activities relevant to a particular product, project, service, or contract.

Quality policy
A quality policy is the overall intentions and directions of an organization regarding quality that were approved by senior management.

Quality surveillance
Quality surveillance is the continuing monitoring and verification of the status of procedures, methods, products, processes, and services to ensure that requirements for quality are being met.

Quality system
A quality system is the organizational structure, procedures, processes, and resources needed to implement quality management. It should be only as comprehensive as needed to meet the quality objectives.

Quality trilogy
The quality trilogy is a three-pronged approach to managing for quality. The three legs include: (1) quality planning (developing the products and processes needed to meet customer needs), (2) quality control (meeting product and process goals), and (3) quality improvement (achieving higher levels of performance).

Quotas
Quotas are legal restrictions on the import quantity of particular goods imposed by governments as barriers to trade.

Random access
Random access is the ability to access a particular data item in a file without having to read through all previous items.

Rapid prototyping
Rapid prototyping is a type of prototyping in which emphasis is placed on developing prototypes early in the development process to permit early feedback and analysis in support of the development process.

Rated capacity
Rated capacity is the expected output capability of a resource or system. It is equal to hours available times efficiency times utilization. It is synonymous with calculated capacity, standing capacity, and nominal capacity. In the theory of constraints, rated capacity is hours available times efficiency times activation, where activation is a function of scheduled production and availability is a function of uptime.

Reality check
The reality check decision is tested in the pseudo–real-world conditions. A T-column is used with headings "Our expectations" and "Our concerns" to facilitate the analysis. It is a decision-making tool.

Recidivism
Recidivism is a tendency to relapse into a previous condition or repeat a mode of behavior.

Record
A record is a unit of related data elements or fields.

Recovery
Recovery is the process of reconstituting a database to its correct and current state following a partial or complete hardware, software, network, operational, or processing error or failure.

Recovery controls
Recovery controls are actions necessary to restore a system's computational and processing capability and data files after a system failure or penetration. Recovery controls for information technology continuity planning are related to recovery point objective and recovery time objective.

Recovery point objective (RPO)
The RPO is point in time in to which data must be recovered after an outage in order to resume computer processing. RPO is a part of information technologycontinuity planning.

Recovery time objective (RTO)
RTO is the overall length of time an information system's components can be in the recovery phase before the organization's mission or business functions are negatively impacted. It is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization. RTO is a part of information technology continuity planning.

Red team
A red team is a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture by conducting penetration testing. The red team's objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and what works for the defenders (i.e., the blue team) in an operational environment. The red team is a test team that performs penetration security testing using covert methods and without the knowledge and consent of the organization's information technology staff but with full knowledge and permission of upper management.

Redundant Array of Independent Disk (RAID)
RAID is a cluster of disks used to back up data onto multiple disk drives at the same time, providing increased data reliability and increased input/output performance. Seven classifications for RAID are numbered as RAID-0 through RAID-6. RAID storage units offer fault-tolerant hardware with varying degrees. Nested or hybrid RAID levels occur with two-deep levels. For example a simple RAID configuration with six disks includes four data disks, one parity disk, and one hot spare disk.

Problems with RAID include correlated failures due to drive mechanical issues, atomic write semantics (meaning that the write of the data either occurred in its entirety or did not occur at all), write cache reliability due to a power outage, hardware incompatibility with software, data recovery in the event of a failed array, untimely drive errors recovery algorithm, increasing recovery times due to increased drive capacity, operator skills in terms of correct replacement and rebuild of failed disks, and exposure to computer viruses. RAID is a part of information technology continuity planning.

Referent power
Referent power is power that results from characteristics that command subordinates' identification with, respect and admiration for, and desire to emulate the leader.

Refreezing
Refreezing is the reinforcement stage of organizational development in which individuals acquire a desired new skill or attitude and are rewarded for it by the organization.

Regiocentric staffing outlook
The regiocentric staffing outlook is a belief that key positions at the regional headquarters should be staffed by individuals from one of the region's countries.

Regional structure
Regional structure is an international corporate structure wherein regional heads are made responsible for specific territories, usually consisting of multiple countries, such as Europe, East Asia, and South America.

Regional trade communities
Regional trade communities are international organizations, conferences, and treaties focusing on business and trade regulations; the European Union is the most prominent of these.

Registration
Registration is a procedure by which a body (entity) indicates relevant characteristics of a product, process, or service and then registers it in an appropriate publicly available list.

Regression testing
Regression testing means rerunning test cases that a program has previously executed correctly in order to detect errors created during software correction or modification activities.

Regulatory arbitrage
Regulatory arbitrage occurs when user organizations take advantage of discrepancies, loopholes, and ambiguities in government laws and regulations.

Release
The term "release" refers to the process of returning all unused disk space to the system when a data set is closed at the end of processing.

Reliability
Reliability is the extent to which a computer system, hardware, or program can be expected to perform its intended function with required precision.

Remediation of threats
Remediation is the act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing patches, adjusting configuration settings, amd uninstalling a software application.

Reorder point
A reorder point is a predetermined inventory level that triggers an order. This level provides inventory to meet anticipated demand during the time it takes to receive the order.

Reorder point system
A reorder point system is a continuous-review inventory control system in which an order is placed whenever a withdrawal brings the inventory position to a predetermined reorder point level.

Repeater
A repeater is a device to amplify the received signals.

Repository
A repository is the database that contains the data.

Request-offer approach
Under the request-offer approach, a contracting party submits requests for concessions on tariff reductions from its trading partner, which, in turn, submits its offer for concessions. The offers are tabled and negotiated by the parties' representatives.

Research virus
A research virus is a virus that has been written but has never been unleashed on the public. These viruses include samples that have been sent to researchers by virus writers.

Resident virus
A resident virus installs itself as part of the operating system upon execution of an infected host program. The virus will remain resident until the system is shut down. Once installed in memory, a resident virus is available to infect all suitable hosts that are accessed. A resident virus loads into memory, hooks one or more interrupts, and remains inactive in memory until some trigger event. When the trigger event occurs, the virus becomes active, either infecting something or causing some other consequence (such as displaying something on the screen). All boot viruses are resident viruses, as are the most common file viruses. Macro viruses are nonresident viruses.

Residual risk
Residual risk is the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk. Residual risk is current risk, which, in turn, is called managed risk with existing control systems. Residual risk is calculated as potential risks minus covered risks, resulting in uncovered risk.
Several equations are available to express residual risks:

Residual risks = Total risks – Mitigated risks
Residual risks = Potential risks – Covered risks
Residual risks = Total risks – Control measures applied
Residual risks = Potential risks – Countermeasures applied
Residual risks = Uncovered or Unaddressed risks

Response time
Response time is the time elapsed between entering a transaction or query and seeing the first character of the system's response appear on a computer or terminal screen.

Restore
A restore is the process of retrieving a data set that has been migrated to offline storage and restoring it to online storage.

Retention program (documents)
A retention program is a management program to save documents, forms, history logs, master and transaction data files, computer programs (both source and object level), and other documents on the system until no longer needed. Retention periods should satisfy organization and legal requirements.

Retroactive pricing
Retroactive pricing is a pricing decision made after some or all of the work specified under contract has been completed, based on a review of performance and recorded cost data.

Reverse marketing or reverse purchasing
In reverse marketing or reverse purchasing, a buyer takes the initiative in making the sourcing proposal to several suppliers in order to find a new supplier. It is a reversal of the traditional buyer/supplier marketing practice where a buyer goes to an existing supplier.

Reward power
Reward power is power that results from the authority to bestow rewards on other people.

Ring
A ring is a topology in which stations are attached to repeaters connected in a closed loop. Two kinds of ring: token ring and bus.

Risk
Risk has several definitions. The term "risk" means the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. It is the probability that an event or action may adversely affect the organization or activity under audit. Risk is uncertainty about loss. Risks should be avoided where possible; if not, they should be managed well. There are at least six specific types of risks, including pure, strategic, operational, financial, hazard, and speculative. Risks can be classified or categorized into three basic categories: static versus dynamic, subjective versus objective, and pure versus speculative.

Risk/exposure
A risk is the probability that an undesirable event will occur, resulting in financial or other loss, or otherwise creating a problem. Exposures are caused by the undesirable events. An example of exposure is the damage (loss of time and integrity of data) that errors (both data and processing) may cause. In other words, the causes must exist before exposures result. In this example, errors must exist before the damages occur.

Risk acceptance
The term "risk acceptance" means accepting a potential risk and continuing with operating a process or system. It is like accepting risks as part of doing business (a kind of self-insurance). Risk acceptance is also called risk tolerance and risk appetite in order to achieve a desired result.

Risk analysis
Risk analysis is: (1) an assessment of the vulnerability of a specific facility or organization to various types of occurrences (e.g., flood, power interruption) that affect their information systems operations; (2) the analysis of possible risks to be encountered and the means to handle them that can be performed. A T-column can be used with headings "Anticipated risks" and "Actions to overcome risks." It is a decision-making tool.

Risk appetite
The risk appetite of an organization is the level of risk that it is willing to accept.

Risk assessment
Risk assessment (or risk analysis) includes identification, analysis, measurement, and prioritization of risks. It is the process of identifying the risks and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Risk assessment is a systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events. The risk assessment process should provide a means of organizing and integrating professional judgments for development of the audit work schedule.

Risk assignment
Risk assignment consists of transferring or assigning risk to a third party by using other options to compensate for the loss, such as an insurance company or outsourcing firm.

Risk avoidance
Risk avoidance eliminates the risk causes and/or consequences (e.g., add controls that prevent the risk from occurring, remove certain functions of the system, or shut down the system when risks are identified). It is like reducing, avoiding, or eliminating risks by implementing

cost-effective safeguards and controls. Risk situations that have high severity and high frequency of loss should be either avoided or reduced. Risk reduction is appropriate when it is possible to reduce either risk severity or frequency. Otherwise, the risk should be avoided or transferred. Examples of risk avoidance controls include (1) separating threats from assets or assets from threats to minimize risks and (2) separating resource allocation from resource use to prevent resource misuse.

Risk control

Risk control identifies the presence or lack of effective controls to prevent, detect, or correct risks. Risk control focuses on minimizing the risk of loss to which an organization is exposed. The situation of high frequency and low severity should be managed with additional controls (loss control). Risk control includes risk avoidance and risk reduction.

Risk engineering

The goal of risk engineering is to reduce risks in traditional and nontraditional insurance activities, which is achieved, in part, through risk financing to fund financial losses. Risk financing includes internal funds for risks (e.g., self-insurance and residual risk) and external transfer of risks (e.g., insurance, hedging, and captive insurance). In a way, risk engineering is related to financial engineering in terms of sharing common goals, such as risks, hedging, insurance, and captive insurance.

Risk financing

Risk financing concentrates on arranging the availability of internal funds to meet occurring financial losses. It also involves external transfer of risk. Risk financing includes risk retention and risk transfer, which is a tool used by captive insurers. Risk retention applies to risks that have a low expected frequency and a low potential severity. Risk transfer applies to risks that have a low expected frequency and a high potential severity (e.g., buying insurance). Insurance should be purchased for losses in excess of a firm's risk retention level.

When losses have both high expected frequency and high potential severity, it is likely that risk retention, risk transfer, and loss control all will need to be used in varying degrees. Common methods of loss control include reducing the probability of losses (i.e., frequency and severity reduction) and decreasing the cost of losses that do occur (i.e., cost reduction). Note that "high" and "low" loss frequency and severity rates are defined differently for different firms.

Risk financing includes internal funding for risks (self-insurance and residual risk) and external transfer of risks, such as insurance and hedging. It can be unfunded or funded retention of risks. The unfunded retention is treated as part of the overall cost of doing business. A firm may decide to practice funded retention by making various pre-loss arrangements to ensure that money is readily available to pay for losses that occur. Examples of funded retention include use of credit, reserve funds, self-insurance, and captive insurers.

Risk limitation

The term "risk limitation" means limiting or containing risks by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, and detective controls) or by authorizing operation for a limited time during which additional risk mitigation efforts by other means is installed.

Risk management

Risk management is the total process of identifying, assessing, controlling, and mitigating risks as it deals with uncertainty. It includes risk assessment (risk analysis); cost/benefit analysis; the selection, implementation, testing, and evaluation of safeguards (risk mitigation); risk financing (risk funding); and risk monitoring (reporting, feedback, and evaluation). It is expressed as:

$$\text{Risk management} = \text{Risk assessment} + \text{Risk mitigation} + \text{Risk financing} + \text{Risk monitoring}$$

The ultimate goal of risk management is to minimize the adverse effects of losses and uncertainty connected with pure risks. Risk management is broken down into two major categories: risk control and risk financing.

Risk mapping
Risk mapping involves profiling risk events to their sources (i.e., threats and vulnerabilities), determining their impact levels (i.e., low, medium, or high), and evaluating the presence of or lack of effective controls to mitigate risks.

Risk mitigation
Risk mitigation involves implementation of preventive, detective, and corrective controls along with management, operational, and technical controls to reduce the effects of risks. It includes designing and implementing controls and control-related procedures to minimize risks.

Risk monitoring
Risk monitoring addresses internal and external reporting and provides feedback into the risk assessment process, continuing the loop.

Risk registers
Risk registers document the risks below the strategic level and include inherent risks (high or higher) and unchanged residual risks, lack of or ineffectiveness of key internal controls, and lack of mitigating factors (e.g., contingency plans and monitoring activities). Risk registers provide direct links among risk categories, risk aspects, audit universe, and internal controls.

Risk retention
Risk retention is retention of risks and is most appropriate for situations in which there is a low probability of occurrence (frequency) with a low potential severity for an event. These are situations that seldom occur, and, when they do happen, the financial impact is small or negligible. Severity dictates whether a risk should be retained. If the potential severity is more than the organization can afford, retention is not recommended. Frequency determines whether the risk is economically insurable. The higher the probabilities of loss, the higher the expected value of loss and the higher the cost of transfer.

Risk spreading or sharing
Risk spreading or sharing involves spreading or sharing risks with other divisions or business units of the same organization. It is viewed as a special case of risk transfer, in which the risk is transferred from an individual to a group, from one division to another, or from one business unit to another. It is a form of risk retention, depending on the success of the risk-sharing arrangement.

Risk transfer
Risk transfer involves payment by one party (the transferor) to another party (the transferee, or risk bearer). The five forms of risk transfer are: (1) hold-harmless agreements, (2) incorporation, (3) diversification, (4) hedging, and (5) insurance. Risk transfer is most likely ideal for a risk with a low expected frequency and a high potential severity.

Rivest-Shamir-Adelman algorithm
The Rivest-Shamir-Adelman (RSA) algorithm is a public-key algorithm used for key establishment and for generation and verification of digital signatures, encrypt messages, and provides key management for the data encryption standard (DES) and other secret key algorithms.

Role-based access control (RBAC) policy
Several definitions exist for RBAC policy. It is: (1) access control based on user roles (e.g., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect

the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals; (2) a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. RBAC is an access control based on specific job titles, functions, roles, and responsibilities.

Roll back
A roll back restores the database from one point in time to an earlier point.

Roll forward
A roll forward restores the database from a point in time when it is known to be correct to a later time.

Root cause
A root cause is a fundamental deficiency that result in a nonconformance, which must be corrected to prevent recurrence.

Root cause analysis
Root cause analysis is a technique used to identify the conditions that initiate the occurrence of an undesired activity or state.

Rootkit
A rootkit is a collection of computer files that is installed on a computer system to alter the standard functionality of the system in a malicious and stealthy way. It is a set of tools used by an attacker after gaining root-level access to a host computer to conceal an attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. Some examples of protection methods against botnets and rootkits include using and maintaining antivirus software, installing a firewall, using strong passwords, updating software with patches, and taking precautions when using e-mails and Web browsers not to trigger an infection.

Router
A router is a physical or logical entity that receives and transmits data packets or establishes logical connections among a diverse set of communicating entities (usually supports both hardwired and wireless communication devices simultaneously).

Rule-based access control policy (RuBAC)
A RuBAC is based on specific rules relating to the nature of the subject and object, beyond its identity, such as a security label. A RuBAC decision requires authorization information and restriction information to compare before any access is granted. RuBAC and mandatory access control policy are considered equivalent.

Rules of behavior
Rules of behavior are rules that are established and implemented concerning use of, security in, and acceptable level of risk in a computer system. They clearly delineate responsibilities and expected behavior of all individuals with access to the system. The organization establishes and makes readily available to all information system these rules, which describes their responsibilities and expected behavior with regard to information system usage. Rules of behavior are established to control the business behavior of employees' on computer systems.

Rules of engagement
Rules of engagement are detailed guidelines and constraints regarding the execution of information security testing. These rules are established before the start of a security test. They give the test team authority to conduct the defined activities without the need for additional permissions. Rules of engagement are established to control the behavior of contractors, vendors, and suppliers during their work for an organization.

Rule set
A rule set is a table of instructions used by a controlled (managed) interface to determine what data are allowable and how the data are handled between interconnected computer systems. Rule sets govern access control functionality of a firewall or a router. The firewall uses these rule sets to determine how packets should be routed between its interfaces. A rule set is a collection of rules or signatures that network traffic or system activity is compared against to determine an action to take, such as forwarding or rejecting a packet, creating an alert, or allowing a system event.

Safeguard rule
A safeguard rule is a temporary import control or other trade restriction that a country imposes to prevent injury to domestic industry from increased imports. It is designed to facilitate the adjustment of domestic industries to the influx of fairly traded imports.

Safe harbor privacy principles
Safe harbor privacy principles are derived from the European Union's comprehensive privacy legislation. They require that transfers of personal data take place only to non–European Union countries that provide an "adequate" level of privacy protection. (Personal data are data about an identified or identifiable individual that are recorded in any form.)

Safer Internet Plus Programme
According to the European Union's Decision 854/2005/EC, it is illegal to post unwanted and harmful content on the Internet. The goal is to keep the Internet safer and is focused on end-users, parents, educators, and children.

Safety capacity
Safety capacity is the planned amount by which the available capacity exceeds current productive capacity. This capacity provides protection from planned activities, such as resource contention, preventive maintenance, and rework.

$$\text{Safety capacity} + \text{Excess capacity} = 100\% \text{ of capacity}$$

Sampling risk
Sampling risk represents the risk that the sample is not representative of the population.

Scanning
Scanning checks computer files for evidence of unauthorized or malicious code. Two types of scanning exist: online scanning and offline scanning. Online scanning checks files as they are created, opened, closed, or executed and is performed by memory resident antivirus software. (Other names for online scanning include automatic, background, resident, and active scanning.) Offline scanning is performed on demand by a user or process. (Other names for offline scanning include manual, foreground, nonresident, and inactive scanning.)

Scavenging of data
Scavenging is searching through residue for the purpose of unauthorized data acquisition.

Scenario analysis
Scenario analysis is a risk analysis technique in which "bad" and "good" sets of financial circumstances are compared with a most likely, or base case, situation.

Scenario building
Scenario building involves the identification of crucial variables and determining their effects on different cases or approaches.

Scenario planning
Scenario planning is a strategic planning process that generates multiple stories about possible future conditions, allowing an organization to look at the potential impact on them and different ways they could respond.

Scenario writing
Scenario writing is a qualitative forecasting method that consists of developing a conceptual scenario of the future based a well-defined set of assumptions.

Schema
A schema is a set of specifications that defines a database. Specifically, it includes entity names, sets, groups, data items, areas, sort sequences, access keys, and security locks.

Secondary storage
Secondary storage consists of nonvolatile, auxiliary memory such as disk or tape/cartridge used for the long-term storage of programs and data.

Secure Sockets Layer (SSL)
SSL is a method for securing information exchange on the Internet. SSL uses data encryption and digital certificate authentication to secure the information exchange.

Seek time
Seek time is the time required to bring the disk/tape drive up to speed and position the access mechanism, such as the disk read/write head, to locate the data or program.

Self-insurance
Self-insurance is a risk-retention program that incorporates elements of the insurance mechanism where the self-insured organization pays the claims rather than an insurance company.

Self-managed team
A self-managed team is a team that requires little supervision and manages itself and the day-to-day work it does; such teams are responsible for whole work processes with each individual performing multiple tasks.

Self-recognition virus
A self-recognition virus uses a procedure is a technique whereby a virus determines whether an executable is already infected. The procedure usually involves searching for a particular value at a known position in the executable. Self-recognition is required if the virus is to avoid multiple infections of a single executable. Multiple infections cause excessive growth in size of infected executables and corresponding excessive storage space, contributing to virus detection.

Sensitive data
Sensitive data are those that require a degree of protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data).

Sensitive system
A sensitive system is a computer system that requires a degree of protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application system.

Sensitivity analysis
Sensitivity analysis: (1) refers to the study of how changes in the probability assessments for the states of nature and/or changes in the payoffs affect the recommended decision alternative; (2) involves using a model to determine the extent to which a change in a factor affects an outcome. The analysis is done by repeating if-then calculations; (3) is a means of incorporating risk in financial outcomes that involves varying key inputs, one at a time, and observing the effect on the decision variable(s). For example, the analyst might vary the sales level and observe the effect on the company's cash forecast.

Sequential access
Sequential access is the ability to access data in a sequential manner (i.e., the order in which it is stored). Files stored in both disk and tape/cartridge media can be sequential.

Serious prejudice in international trade agreements
Under the proposed subsidies agreement, there would be a special category of actionable subsidies that would have a high likelihood of being trade distorting. The proposed agreement lays out specific criteria for demonstrating when a country's use of such subsidies would have adversely affected another country's trade interests through price or volume/market share effects (referred to in the agreement as "serious prejudice"). The proposed agreement would create an obligation to withdraw the subsidy or remove the adverse effects when they are identified.

Servant leader
A servant leader is a leader who works to fulfill subordinates' needs and goals as well as to achieve the organization's larger mission.

Server mirroring
The purpose of server mirroring is same as disk arrays, but a file server is duplicated instead of a disk. All information is written to both servers simultaneously to backup data.

Service
Service is a result generated by activities and the interface between the supplier and the customer and by supplier internal activities to meet the customer needs. An organization can have both internal and external suppliers and customers.

Service-level agreements (SLAs)
SLAs between service providers and receivers should, as a minimum, specify these points:

- Explicit definitions of both the user organization's roles and responsibilities and the service provider's roles and responsibilities.
- Period of performance and/or deliverables due dates.
- Defined service levels and their costs.
- Defined processes regarding how the managers will assess the service provider's compliance with the service level and due date targets, rules, laws, regulations, and performance levels.
- Specific remedies (e.g., financial, technical, and legal) for noncompliance or harm caused by the service provider.
- Explicit rules and processes for handling sensitive data to ensure privacy.

Services
Services, as defined in the Trade and Tariff Act of 1984, consists of economic activities whose outputs are other than tangible goods, including businesses such as accounting, advertising, banking, engineering, insurance, management consulting, retail, tourism, transportation, and wholesale trade.

Seven tools of quality control
The seven tools of quality control are tools that help organizations understand their processes in order to improve them. The seven tools are the cause-and-effect diagram, checksheet, control chart, flowchart, histogram, Pareto chart, and scatter diagram. These seven old tools can also be used to solve problems.

Seven tools of quality management
The seven tools of quality management is a series of tools to help quality management understand the processes and data better. The seven tools are affinity diagram (also called KJ method), tree diagram, process decision program chart, matrix diagram, interelationship digraph, prioritization matrices, and activity network diagram. These seven tools are also called quality planning tools. The quality management tools were introduced after the quality control tools.

Shareware
Shareware is software that is distributed free of charge, often through electronic bulletin boards, may be freely copied, and for which a nominal fee is requested if the program is found useful].

Shoulder surfing
Shoulder surfing involves stealing passwords or personal identification numbers by looking over someone's shoulder.

Sign-off
Functional users are requested and required to approve in writing their acceptance of the system at various stages or phases of the system development life cycle.

Situation analysis
Situation analysis is an analysis of the strengths, weaknesses, opportunities, and threats (SWOT) that affect organizational performance.

Situational ethics
Situational ethics is a societal condition where "right" and "wrong" are determined by the specific situation rather than by universal moral principles.

Situational leadership
Situational leadership is a leadership theory that maintains that the leadership style should change based on the person and the situation, with the leader displaying varying degrees of directive and supportive behavior.

Situational theory
Situational theory is a contingency approach to leadership that links the leader's behavioral style with the task readiness of subordinates.

Six Sigma
Six Sigma is an approach to measuring and improving product and service quality. In Six Sigma terminology, a defect (nonconformance) is any mistake or error that is passed on to the customer. Six Sigma represents a quality level of at most 3.4 defects per million opportunities. Its goal is to find and eliminate causes of errors or defects in processes by focusing on characteristics that are critical to customers.

Six Sigma players
Several Six Sigma players exist in the planning and implementation of a Six Sigma program in an organization, including white belts (at the bottom), green belts, black belts, master black belts, project champions, and senior champions (at the top). All these players assume defined roles and responsibilities and need specific training of varying lengths to make the Six Sigma program a success, as follows:

White belts are hourly employees needing basic training in Six Sigma goals, tools, and techniques to help green belts and black belts on their projects.

Green belts are salaried employees who have a dual responsibility in implementing Six Sigma in their function and carrying out their regular duties in that function. They gather and analyze data in support of a black belt project and receive a simplified version of black belt training.

Yellow belts are seasoned salaried employees who are familiar with quality improvement processes.

Black belts are salaried employees who have a full-time responsibility in implementing Six Sigma projects. They require hard skills and receive extensive training in statistics and problem-solving and decision-making tools and techniques, as they train green belts. Black belts are very important to Six Sigma's success.

Master black belts are salaried employees who have a full-time responsibility in implementing Six Sigma projects. They require soft skills, need some knowledge in statistics, and need more knowledge in problem-solving and decision-making tools and techniques, as they train black belts and green belts.

Small power distance culture

A small power distance culture is a culture where employees perceive few power differences and follow a superior's instructions only when they either agree or feel threatened.

Smart card

A smart card is a credit card–size card with embedded integrated circuits that can store, process, and communicate information. It has a built-in microprocessor and memory that is used for identification of individuals or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

Social engineering

Social engineering is a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Some spyware software can trick users to run or install malware. Examples of social engineering include pretexting, phishing, and pharming activities. The best control is to exercise caution when downloading anything from public Web sites, newsgroups, Instant Messaging sessions, or when opening e-mail attachments from unknown persons.

Software hole

A software hole (weakness) penetrates a computer system due to a lack of perimeter defenses, which is risky. The software hole can reside in any of the three layers (i.e., networking, operating system, or application). The software vendor or developer should provide security mechanisms to mitigate the risks of such holes. Defending the perimeter requires installing appropriate security controls at all entry points into the network, including the Internet connection. Testing the perimeter to identify backdoors and software holes requires table-top reviews, periodic assessments, war-dialing, war-driving, wireless scanning, and penetration testing.

Source code/module

Source code/module is the form of software used by programmers to create and modify software.

Source code escrow

Source code escrow is an arrangement with a third party (e.g., a bank) to hold the software under its custody and make it available to user organizations under unusual business circumstances. This arrangement is applicable to vendor-developed applications software packages either purchased or leased by user organizations. Usually vendors do not give the source code to users, which is risky.

Source code virus

Visual Basic programming language is a good target for a source code virus where it looks for file extensions such as .C and .BAS.

Spamming
Spamming refers to posing identical messages to multiple unrelated newsgroups on the Internet (e.g., USENET). It is often used as cheap advertising, to promote pyramid schemes, or simply to annoy other people.

Special economic zones
Special economic zones are areas created by a country to attract foreign investors. In the zones, there are no tariffs and there are substantial tax incentives and low prices for land and labor.

Special-purpose team
A special-purpose team is an organizational team formed to address specific problems, improve work processes, and enhance product and service quality.

Specification
A specification is a requirement with which a product or service must conform.

Specificity provision in agreements
Under the proposed subsidies agreement, subsidies must be "specific" in order to be actionable. A subsidy is considered "specific" to a firm or an industry, or a group of firms or industries, if the government limits access to the assistance in law or in fact.

Speculative buying
The term "speculative buying" refers to purchasing material in excess of current and future known requirements, with the intention of profiting on price movement.

Speculative risk
Speculative risk exists when there is uncertainty about an event that could produce either a profit or a loss. It involves the chance of loss or gain (e.g., hedging, options, and derivatives).

Split knowledge
Split knowledge is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to re-create the original cryptographic key. It is the separation of data into two or more parts, with each part constantly kept under control of separate authorized individuals or teams so that no one individual will be knowledgeable of the total data involved. It is similar to using a dual control mechanism.

Spoofing
Spoofing is the deliberate inducement of a user or a resource to take an incorrect action. Many spoofing attacks exist. An example is the Internet Protocol spoofing attack, in which a network packet that appears to come from a source other than its actual source is sent. Spoofing involves the ability to receive a message by masquerading as the legitimate receiving destination or masquerading as the sending machine and sending a message to a destination.

Spooling
On input, the term "spooling" refers to transferring data to secondary storage and holding them for eventual processing. On output, "spooling" refers to transferring data to secondary storage for eventual output. It is a technique used to make batch processing applications more efficient.

Spot market
A spot market is a financial market where buying and selling of foreign exchange takes place or where currencies are traded for current delivery on the spot.

Spread
Spread is the difference between selling and buying rates of a foreign exchange. It is a financial market.

Spyware
Spyware is adware that tracks user activity and passes it to third parties without the user's knowledge or consent. Its intent is to violate a user's privacy. Types of spyware include web bugs, which are tiny graphics on a Web site that are referenced within the Hypertext Markup Language (HTML) content of a Web page or e-mail to collect information about the user viewing the HTML content, and tracking cookies, which are placed on the user's computer to track activity on different Web sites and create a detailed profile of the user's behavior. To combat spyware, install an antispyware software, which is a program that specializes in detecting both malware and nonmalware forms of spyware.

Stackguarding technology
Stackguarding technology uses a layered defense approach, which makes it extremely difficult for attackers to exploit computer buffer overflows, the most common type of vulnerability discovered in network code. Stackguarding can also prevent worms from gaining increased privileges on that system. Worms that gain control of a low-privilege account may attempt to elevate their privilege. Hence, stackguarding can defend against buffer overflow and worm attacks.

Stages of team growth
The term "stages of team growth" refers to four development stages through which groups typically progress: forming, storming, norming, and performing. Knowledge of the stages helps team members accept the normal problems that occur on the path from forming a group to becoming a team.

Stakeholder audit
A stakeholder audit is a systematic attempt to identify and measure issues of an organization's stakeholders and measure and evaluate their opinions with respect to their effective resolution.

Stakeholder environment
A stakeholder environment is composed of trends, events, issues, expectations, and forecasts that may have a bearing on the strategic management process and the development of corporate public policy.

Stakeholders
Stakeholders are individuals or entities that have an interest in the well-being of a firm—stockholders, creditors, employees, customers, suppliers, and so on.

Standard of review
A standard of review refers to the criteria that dispute panels use to determine the merits of a given case. The standard is used to define the appropriate level of review, given the issues involved in that case.

Standing
Standing refers to whether a party has a sufficient stake in an otherwise justifiable controversy to obtain judicial resolution of that controversy. With regard to antidumping proceedings under the General Agreement on Tariffs and Trade or World Trade Organization, standing refers to the right of a party or parties in the importing country to petition for relief under national antidumping laws or to support a petition.

Star
A star is a topology in which all stations are connected to a central switch.

Static gains
Static gains stem from the increased efficiency of resource allocation and improved consumption possibilities. Additional gains from trade may result from increasing returns to scale and from increased product and input variety for consumers and producers. Static gains imply a

change in the amount of aggregate output but not its growth rate. In empirical studies of trade liberalization, static gains from trade are relatively small as a percentage of gross domestic product.

Static risk
Static risk, which can be either pure or speculative, stems from an unchanging society that is in stable equilibrium. Examples of pure static risk include the uncertainties due to such random events as lightning, windstorms, and death. Business undertakings in a stable economy illustrate the concept of speculative static risk.

Station
A station is one of the input or output points of a telecommunication system (e.g., telephone set, terminal, computer).

Stealth virus
A stealth virus is a resident virus that attempts to evade detection by concealing its presence in infected files. To achieve this, the virus intercepts system calls that examine the contents or attributes of infected files. The results of these calls must be altered to correspond to the file's original state. For example, a stealth virus might remove the virus code from an executable when it is read (rather than executed) so that an antivirus software package examines the original, uninfected host program. A stealth virus uses any of a variety of techniques to make itself more difficult to detect. For example, a stealth boot virus typically intercepts attempts to view the sector in which it resides and instead shows the viewing program a copy of the sector as it looked prior to infection. An active stealth file virus typically does not reveal any size increase in infected files when a user issues the DIR command. Stealth viruses must be active, or running, in order to exhibit their stealth qualities.

Steering committee
A steering committee is a group of management representatives from each user area of information systems services that establishes plans and priorities and reviews project's progress and problems for the purpose of making management decisions.

Stockholders
Stockholders and shareholders are owners of a corporation.

Stockless purchasing
Stockless purchasing is an arrangement where a supplier holds inventory until the buyer places orders for specific items. Examples include blanket orders, open-end orders, and system contracts.

Store and forward
The term "store and forward" refers to the interruption of data flow from the originating terminal to the designated receiver by storing the information en route and forwarding it at a later time.

Storming
Storming is the stage of team development in which individual personalities and roles, and resulting conflicts, emerge.

Storyboard
A storyboard is a group problem-solving technique to create a picture of relevant information. A storyboard can be created for each group that is making decisions.

Storyboarding
Storyboarding is a technique that visually displays thoughts and ideas and groups them into categories, making all aspects of a process visible at once. Often it is used to communicate to

others the activities performed by a team as they improved a process. A positive outcome of storyboarding is that it takes less time than interviewing, and many employees can get involved in problem solving, not just managers.

Strategic activities
Strategic activities are those activities that support the long-term objectives of an organization. Examples include strategic planning and strategic sourcing.

Strategic advantage
Strategic advantage is a position in which one dominates a market; also called competitive advantage.

Strategic alliance
A strategic alliance: (1) is a firm's collaboration with companies in other countries to share rights and responsibilities as well as revenues and expenses as defined in a written agreement. Some common types of strategic alliances are research collaboration, a licensing program, and a copromotion deal; (2) two or more companies that band together to attain efficiency. *See* Joint venture.

Strategic business unit (SBU)
An SBU is a division of the organization that has a unique business mission, product line, competitors, and markets relative to other SBUs in the same corporation.

Strategic fit review
A strategic fit review is a process by which senior managers assess the future of each project of an organization in terms of its ability to advance the mission and goals of that organization.

Strategic goals
Strategic goals are broad statements of where the organization wants to be in the future; they pertain to the organization as a whole rather than to specific divisions or departments.

Strategic human resource management
Strategic human resource management is the organizational use of employees to gain or keep a competitive advantage against competitors.

Strategic information system
A strategic information system is any information system that gives its owner a competitive advantage.

Strategic leader
A strategic leader is a highly competent firm located in a strategically critical market.

Strategic management
Strategic management is the set of decisions and actions used to formulate and implement strategies that will provide a competitively superior fit between the organization and its environment so as to achieve organizational goals.

Strategic manager
A strategic manager is a person who makes decisions that affect an entire organization, or large parts of it, and leaves an impact in the long run.

Strategic marketing concept
A strategic marketing concept states the company's mission to identify, generate, and sustain competitive advantage through superior positioning and vision.

Strategic objectives
Guided by the enterprise's mission or purpose, strategic objectives associate the enterprise with its external environment and provide management with a basis for comparing performance with that of its competitors, in relation to environmental demands.

Strategic plan
A strategic plan is a plan that integrates an organization's major goals, policies, and action sequences into a cohesive whole. It is the action steps by which an organization intends to attain its strategic goals.

Strategic planning
Strategic planning is a process to set an organization's long-range goals and identify the actions needed to reach the goals.

Strategic risk
Strategic risk is a high-level and corporate-wide risk, which includes strategy risk, political risk, economic risk, regulatory risk, reputation risk, global risk, leadership risk, customer risk, and market brand management risk. It is also related to failure of strategy and changing customer needs and business conditions.

Strategy
A strategy is the plan of action that prescribes resource allocation and other activities for dealing with the environment and helping the organization attain its goals.

Strategy formulation
Strategy formulation is the stage of strategic management that involves the planning and decision making that lead to the establishment of the organization's goals and of a specific strategic plan.

Strategy implementation
Strategy implementation is the stage of strategic management that involves the use of managerial and organizational tools to direct resources toward achieving strategic outcomes.

Stress testing of application programs
Computer application programs are tested with test data chosen for maximum, minimum, and trivial values, or parameters.

Stretch goal
A stretch goal is one that requires a significant change in the performance (quality, quantity, time, cost) of a process. It forces an organization to think in a radically different way for major and incremental improvements.

Striking price
A striking price is the price at which currency can be bought or sold. In a financial market.

Strong authentication
Strong authentication requires the use of multiple factors for authentication using and advanced technology (i.e., dynamic passwords or digital certificates) to verify an entity's identity.

Structured techniques
Structured techniques are an orderly and systematic process that shows interrelationships of activities among all functions of a system and among programs, input data, and output reports. The techniques begin system analysis by specifying user system (output) needs first and then working backward to input data. Structured techniques can be applied to system requirements, design, programming, and testing activities. They can produce small, quality program modules that are easy to maintain.

Stub
A stub is a special code segments that, when invoked by a code segment under test, will simulate the behavior of designed and specified modules not yet constructed.

Subject
A subject is an active entity, generally in the form of a person or process, that causes information to flow among objects or changes the system state.

Subjective risk
"Subjective risk" refers to the mental state of an individual who experiences doubt or worry as to the outcome of a given event. In addition to being subjective, a particular risk may be either pure or speculative and either static or dynamic.

Subroutine
A subroutine is a computer program that can be used frequently or referenced by other programs.

Subschema
A subschema is a subset of a schema. It represents a portion of a database as it appears to a user or application program.

Subsidy
A subsidy is generally considered to be a bounty or a grant provided by a government that confers a financial benefit on the production, manufacture, or distribution of goods or services. Government subsidies include direct cash grants, concessionary loans, loan guarantees, and tax credits.

Substantive auditing or testing
Substantive auditing or testing is the process of verifying specific transactions, balance sheet and income statement account values, amounts, and their relationships. Compliance auditing or testing should precede substantive auditing or testing because compliance audits set the scope for substantive audits.

Success-failure analysis
Success-failure analysis is a qualitative approach to brainstorm conditions for both success and failure. A T-column can be used with headings "What will guarantee success" and "What will guarantee failure." It is a decision-making tool.

Sunset
The term "sunset" refers to the duration of antidumping or countervailing duty orders.

Supervisor call (SVC)
SVC is an assembler language instruction that causes a hardware interruption when executed. The operating system then passes control to a program referred to as an SVC. When a program calls SVC, a list of parameters is passed to the SVC to tell the operating system what system service is being requested (allocating a data set, opening and closing files). Operating system components or modules that perform these services must often run in supervisor state or the master storage key so they can update system control blocks. The SVC instruction lets them do this, even when they are called from an unauthorized program.

Supervisor state
The supervisor state is one of two generally possible states in which a computer system may operate and in which only certain privileged instructions may be executed. The other state in which a computer system may operate is the problem state, in which privileged instructions may not be executed. The distinction between supervisor and problem state is key to the integrity of the system.

Supplier partnership
A supplier partnership is a business relationship between a supplying firm and a buying firm for mutual benefit of both parties. It requires a commitment, trust, and a common direction for the future. It is not a legal partnership but a strategic alliance.

Supply chain
A supply chain is a series of firms providing value-added activities from raw materials to finished goods purchased by a final customer. From an information technology viewpoint, it is a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier/producer to consumer/customer. It involves several layers of suppliers. The scope can domestic or international in nature, and it uses a defense-in-breadth strategy. It can be risky because several suppliers are involved.

Sustainable competitive advantage
A sustainable competitive advantage is a competitive edge that cannot be easily or quickly copied by competitors in the short run.

Sustainable growth
Sustainable growth is the rate of sales growth that is compatible with a firm's established financial policies including asset turnover, net profit margin, dividend payout, and debt to equity ratio. It assumes that new equity is derived only through retained earnings, not new common stock.

SWOT analysis
SWOT analysis is an assessment of an organization's key strengths, weaknesses, opportunities, and threats. It considers factors such as the organization's industry, its competitive position, functional areas, and management. SWOT analysis is useful in developing an organization's strategy and is same as situation analysis.

Synchronous communication
Synchronous communication is the transmission of data at very high speeds using circuits in which the transfer of data is synchronized by electronic clock signals. Synchronous communication is used within the computer and in high-speed mainframe computer networks.

Synectics
Synectics is a technique for creating an environment that encourages creative approaches to problem solving. It is a problem-solving tool.

System development life cycle (SDLC)
SDLC is a systematic process for planning, analyzing, designing, developing, implementing, operating, and maintaining a computer-based application system.

System integrity
System integrity is the condition that exists when there is complete assurance that any program not authorized by a mechanism under the installation's control cannot (1) circumvent or disable store or fetch protection, (2) access a protected resource, and (3) obtain control in authorized (supervisor) state. Also, it is the state that exists when there is complete assurance that under all conditions a computer system is based on (1) the logical correctness and reliability of the operating system, (2) the logical completeness of the hardware and software that implement the protection mechanisms, and (3) data integrity.

System integrity exposure
System integrity exposure is a condition that exists when there is a potential of one or more programs that can bypass the installation's control and (1) circumvent or disable store or fetch protection, (2) access a protected resource, and (3) obtain control in authorized (supervisor) state. This condition can lead to compromise of systems protection mechanisms and data integrity.

Systems contract
A systems contract is a contract generated by the purchasing department that authorizes designated employees of the buying firm to place orders directly with the supplier. A release system is developed for specific materials during a given contract period.

System software
System software is the operating system and accompanying utility programs that enable a user to control, configure, and maintain the computer system, software, and data.

Tactical goals
Tactical goals are goals that define the outcomes that major divisions and departments must achieve in order for the organization to reach its overall goals.

Tactical managers
Tactical managers are individuals who receive general directions and goals from their superiors and, within those guidelines, make decisions for their subordinates; also called middle managers.

Tactical objectives
Tactical objectives are objectives that, guided by the enterprise's strategic objectives, identify the key result areas in which specific performance is essential for the success of the enterprise and aim to attain internal efficiency.

Tactical plans
Tactical plans are short-term plans, usually of one- to two-year duration, that describe actions the organization will take to meet its strategic business plan.

Tactics
Tactics are strategies and processes that help an organization meet its objectives.

Taguchi methodology
Taguchi methodology is a concept of offline quality control methods conducted at the product and process design stages in the product development cycle. It encompasses three phases of product design: system design, parameter design, and tolerance design. The goal is to reduce quality loss by reducing the variability of the product's characteristics during the parameter phase of product development. The method is named after a Japanese engineer.

Tall structure
A tall structure is a management structure characterized by an overall narrow span of management and a relatively large number of hierarchical levels.

T-analysis
T-analysis is a tabular presentation of strengths on one side and weaknesses on the other side of the letter "T." The goal is to address the weaknesses (problems). It is a problem-solving tool.

Tap
A tap is an analog device that permits signals to be inserted or removed from a twisted pair or coaxial cable.

Tape library
A tape library is a physical room where a librarian issues, records, controls, and maintains records on the movement of tapes, disks, diskettes, cartridges, and documents.

Target marketing
Target marketing involves promoting products and services to the people who are most likely to purchase them.

Target markets
Target markets are market segments whose needs and demands a company seeks to serve and satisfy.

Target pricing
In target pricing, a buying organization estimates the highest price it could pay to a supplier and still sell its product competitively in the marketplace. Further negotiations between the two parties can bring costs and prices down.

Tariff
A tariff is a tax placed on imported goods to raise revenues and protect domestic industries from foreign competition.

Tariff escalation
Tariff escalation occurs whenever a country imposes substantially higher duties on partially and fully processed goods than on their underlying raw materials.

Tariff peak
A tariff peak is a tariff above 15%.

Tariff reduction
Tariff reduction occurs when tariffs are assigned relative weights based on their value, and those weights are totaled and then averaged to achieve a single overall reduction amount.

Tariff schedules
Tariff schedules are long lists of products containing various tariff rates. Each contracting party is committed not to raise its tariffs above the duty level contained in the schedule. The General Agreement on Tariffs and Trade and World Trade Organization consisted both of schedules of tariff commitments, one for each of the contracting parties, and a set of rules drafted primarily to protect the evasion of tariff commitments.

Task force
A task force is a temporary team or committee formed to solve a specific short-term problem involving several departments.

Task identity
Task identity is the extent to which the job includes a "whole" identifiable unit of work that is carried out from start to finish and that results in a visible outcome.

Task significance
Task significance is the impact the job has on other people.

Task specialist role
A task specialist role is a role in which an individual devotes personal time and energy to helping the team accomplish its task.

Team
A team is a set of two or more people who are equally accountable for the accomplishment of a purpose and specific performance goals; it is also defined as a small number of people with complementary skills who are committed to a common purpose. Many organizations manage themselves through empowered self-managed teams.

Team-based structure
A team-based structure is: (1) an organizational structure in which team members are organized around performing a specific function of the business, such as handling customer complaints or assembling an engine; (2) a structure in which the entire organization is made up of teams that coordinate their work and work directly with customers to accomplish the organization's goals.

Team building
Team building is a: (1) process that enhances the cohesiveness of a department or group by helping members learn how to organize their work and assume responsibility for it; (2) type of organizational development intervention that enhances the cohesiveness of departments by helping members learn to function as a team.

Team building/development
Team building/development is a process of transforming a group of people into a team and developing the team to achieve its purpose.

Team cohesiveness
Team cohesiveness is the extent to which team members are attracted to the team and motivated to remain in it.

Team dynamics
The term "team dynamics" refers to the interactions that occur among team members under different conditions.

Team facilitation
Team facilitation deals with both the role of the facilitator on the team and the techniques and tools for facilitating the team.

Team interview
Team interview is an interview in which the team members with whom they will work interview applicants.

Team performance evaluation, rewards, and recognition
Special metrics are needed to evaluate the work of a team (to avoid focus on any individual on the team) and as a basis for rewards and recognition for team achievements.

Teleprocessing monitor
A teleprocessing monitor is a systems software product that allows a terminal to communicate with an application program.

Test driver
A test driver is a program that directs the execution of another program against a collection of test data sets.

Theoretical capacity
Theoretical capacity is the maximum output capability, allowing no adjustments for preventive maintenance, machine downtime, and plant shutdown.

Theory of constraints
The theory of constraints is a management philosophy applied to manufacturing operations that can be viewed as three separate but interrelated areas: logistics, performance measurement, and logical thinking. Logistics include drum-buffer-rope schedule, buffer management, and logical product structure. Performance measurement includes throughput, inventory, and operating expenses. Logical thinking tools are important in identifying the root problem (current reality tree), identifying and expanding win-win solutions, and developing implementation plans.

Third-country dumping
Third-country dumping occurs when country X dumps its products in country Y and causes injury to country Z's producers, who are competing for the same market but at "fair" prices.

Thrashing
Thrashing is a situation that occurs when paging on a virtual memory system is so frequent that little time is left for useful work.

Threat
A threat is a potential violation of system security. It is any circumstance with the potential to cause loss or harm. Threats arise from internal failures, human errors, attacks, and natural catastrophes.

Throughput
Throughput can be defined in a number of ways. (1) Machine throughput is the central processing unit run time divided by elapsed time. (2) Job throughput is the actual number of jobs processed during a specific period by the elapsed time. (3) Throughput is the total volume of production through a facility (machine, work center, department, plant, or network of plants). (3) In the theory of constraints, it is the rate at which the system (firm) generates money through sales. Throughput is a separate concept from output.

Throughput time
Throughput time is the total time required in processing a queue from concept to launch, from order received to delivery, or from raw materials received to delivery to customer.

Tiger team
A tiger team is an old name for a red team, in information technology testing but some organizations still use it for a different purpose, as follows. For example, in a product development strategy, the tiger team must:

- Understand business use cases and abstract models of a product.
- Develop functional requirements based on the business use cases and abstract models.
- Translate functional requirements into technical standards.

Time-based competition
Time-based competition is a competitive strategy based on the ability to deliver products and services faster than competitors.

Time bomb
A time bomb is a resident computer program that triggers an unauthorized or damaging action at a predefined time.

Time to recover
Time to recover (TTR) is the time required for any computer resources to be recovered from disruptive events. It is the time required to reestablish an activity from an emergency or degraded mode to a normal mode. It is also defined as emergency response time (EMRT).

To-be process model
The to-be process model is a process model that results from a business process redesign/reengineering action. It shows how the business process will function after the improvement action is implemented.

Tokyo Round codes
The Tokyo Round codes are an extension of General Agreement on Tariffs and Trade or World Trade Organization in that they explicitly extend trade discipline in specific new areas or define more precisely existing discipline and rules. The difference between the GATT approach and the Tokyo Round codes' approach is one of degree. In large part the codes are used because amending GATT has proven difficult.

Top-down approach
A top-down approach is an approach that starts with the highest-level component of a hierarchy and proceeds through progressively lower levels.

Topology
Topology is the structure, consisting of paths and switches, that provides the communications interconnection among nodes of a network.

Total factor productivity
The total factor productivity is a measure of the productivity of a department, plant, strategic business unit, or firm that combines the individual productivities of all its resources including labor, capital, energy, material, and equipment. For example, if material accounts for 50% of the cost of sales, labor 15% of the cost of sales, equipment 20% of the cost of sales, capital 10% of the cost of sales, and energy 5% of the cost of sales:

$$\begin{aligned}\text{Total factor productivity} = {} & 0.50\ (\text{Material productivity}) + 0.15\ (\text{Labor productivity}) \\ & + 0.20\ (\text{Equipment productivity}) + 0.10\ (\text{Capital productivity}) \\ & + 0.05\ (\text{Energy productivity})\end{aligned}$$

Total quality management (TQM)
TQM is a management approach based on participation of all employees that aims at long-term success through customer satisfaction and benefits to the organization.

Traceability
Traceability is the ability to trace the history, application, or location of an entity by means of recorded identification.

Tracing
Tracing is an automated procedure performed by software that shows what program instructions have been executed in a computer program and in which sequence they have been executed. Tracing can also be performed manually by following the path of a transaction or an activity from beginning to the end and vice versa.

Trade-balancing requirements
Trade-balancing requirements allow an investor to import goods only up to a specified amount, which is determined by the investor's locally produced exports. Governments use such requirements in an effort to maintain or achieve a favorable balance of trade.

Trademark
A trademark is a mark that manufacturers or merchants use to identify their goods and distinguish them from others. Service marks perform the same function for services. Examples of these marks include personal names, letters, numerals, figurative elements, and combination of colors.

Trade-Related Investment Measures (TRIMs)
TRIMs are placed on foreign direct investment by governments in an effort to influence investment decisions, such as sourcing, production, and market locations, and to increase the likelihood that the host nation will capture the benefits expected from the investment. TRIMs can be mandatory or can take an incentive form as actions that are necessary for an investor to undertake in order to obtain some type of advantage. TRIMs require specific behavior from investors that has an effect on trade.

Trade secret
A trade secret is proprietary information that is used in industry or commerce. Trade secret protection can encompass a broad range of manufacturing processes, testing, materials, and other

know-how making up the most valuable resources a company has to license. This protection is regarded as vital to the coverage of new technology, particularly technology that may not satisfy the rigorous standards of patentability.

Trade-weighted basis
The trade-weighted basis is the average tariff computed by weighing each tariff rate by the dollar value of imports at that rate relative to the total value of imports. Tariffs on individual commodities in the Uruguay Round agreement were reduced sufficiently such that the new tariff schedule would result in a total trade-weighted tariff reduction of 33%. Individual commodity tariffs were not equally affected, however, as many would be reduced to zero, while others would be left unchanged.

Transaction
A transaction is a logical unit of work for an end user. Also, the term is used to define a program or a dialog in a computer system.

Transactional leader
A transactional leader is a leader who clarifies subordinates' role and task requirements, initiates structure, provides rewards, and displays consideration for subordinates.

Transactional leadership
Transactional leadership is a style of leading whereby the leader sees the work as being done through clear definitions of tasks and responsibilities and the provision of resources as needed.

Transborder data flow
Transborder data flow deals with the movement and storage of data by automatic means across national or federal boundaries. It may require data encryption when data are flowing over some borders or countries.

Transformational leader
A transformational leader is a leader distinguished by a special ability to bring about innovation and change.

Transformational leadership
Transformational leadership is a style of leading whereby the leader articulates the vision and values necessary for the organization to succeed.

Transmission medium
A transmission medium is the physical path between transmitters and receivers in a communication network.

Transnational corporation (TNC)
The term favored by the United Nations as an alternative to the term *multinational corporation (MNC)*.

Transnational strategy
A transnational strategy is a strategy that combines global coordination to attain efficiency with flexibility to meet specific needs in various countries. It is the same as *global strategy*.

Transparency
Transparency refers to the extent to which laws, regulations, agreements, and practices affecting international trade are open, clear, measurable, and verifiable.

Transceiver
A transceiver is a terminal that can transmit and receive traffic. It is used in local area networks.

Transponder
A transponder is a device used in a data communications satellite that receives a signal from a sending earth station and retransmits the signal to one or more receiving earth stations.

Tree
A tree is a topology in which stations are attached to a shared transmission medium.

TRIZ
TRIZ is a theory of solving inventive problems, and it is a Russian acronym. It supports the idea that unsolved problems are the result of contradicting goals (constraints) and nonproductive thinking. It suggests breaking out of the nonproductive thinking mold by reframing the contradicting and competing goals in such a way that the contradictions disappear. It is a problem-solving tool.

Systems analysis
Systems analysis breaks down a large problem into many smaller problems. It is an excellent technique if the desired outcome of the problem-solving session is a detailed understanding of a problem. It is a problem-solving tool.

Trojan horse
A Trojan horse is a computer program in which malicious or harmful programming code is packaged inside apparently harmless software or data.

Tuple
A tuple is a row of a relational table.

Turnaround time
Turnaround time is the time between job submission and job completion.

Twisted pair
Twisted pair is an electromagnetic transmission medium consisting of two insulated wires arranged in a regular spiral patterns.

Two-bin system
A two-bin system is a simple, manual inventory system in which an item's inventory is stored in two different locations, with the first bin being the place where inventory is first withdrawn. When the first bin becomes empty, the second bin provides backup to cover the demand until a replenishment order arrives.

Two-tiered pricing
Two-tiered pricing occurs when a government charges a higher price for export than for domestic sales of a scarce natural resource input, thereby providing a competitive advantage to a domestic industry using this input.

Uncertainty
Managers know what goal they wish to achieve, but information about alternatives and future events is incomplete.

Uncertainty acceptance
Uncertainty acceptance is the extent to which uncertainty is considered a normal part of life; feeling comfortable with ambiguity and unfamiliar risks.

Uncertainty avoidance
Uncertainty avoidance is: (1) a value characterized by people's intolerance for uncertainty and ambiguity and their resulting support for beliefs that promise certainty and conformity; (2) a dimension of culture that refers to the preference of people in a country for structured rather than unstructured situations.

Unfair trade practices
Unfair trade practices include the dumping of an exported product below the price charged for the same good in the "home" market of the exporter or the subsidizing of a product by a government.

Unfreezing
Unfreezing is a stage of organizational development in which participants are made aware of problems in order to increase their willingness to change their behavior.

Unit testing
Unit testing is the compilation, execution, and testing of each source program with its test data.

United States Foreign Corrupt Practices Act (FCPA)
The FCPA is an act that makes it illegal for U.S. citizens and businesses to practice bribery in the conduct of business not only in the United States but in other countries as well, even when it is an acceptable or expected business practice there.

Uruguay Round
The Uruguay Round was the eighth and most recent round of multilateral trade negotiations held under the auspices of the General Agreement on Tariffs and Trade (GATT). These negotiations were initiated in Uruguay in September 1986 and concluded in April 1994. That month GATT member-nation officials signed the Uruguay Round as the "Final Act."

Utilitarian approach
The utilitarian approach is an ethical concept that moral behaviors produce the greatest good for the greatest number.

Utility program
A utility program is a computer program or routine that performs general data and system related functions required by other application software, the operating system, or users. Examples include copy, sort, and merge files.

Validation
Validation is the process of evaluating software to ensure compliance with software requirements and correctness. In general, it is the process of evaluating an activity to ensure compliance with specified requirements.

Valuation
Valuation is a process of verifying that a recorded financial amount fairly represents an item's (e.g., equipment, inventory, furniture) real worth considering the market, cost, and economic and political conditions.

Value added
Value added in business processes are those activities or steps that add to or change a product or service as it goes through a process; these are the activities or steps that customers view as important and necessary.

Value-added network (VAN)
A VAN is a network of computers owned or controlled by a single entity that can be used by subscribers for data transmission, e-mail, information retrieval, and other functions.

Value analysis
Value analysis is a systematic study of a business process or product with a view to improving the process or product and reducing cost. Creative skills are required while doing value analysis. Its goal is to ensure that right activities are performed in the right way the first time. Industrial engineering techniques, such as work measurement and simplification methods,

can be used to achieve the goals. It is a group approach that encourages free discussion and exchange of ideas is required to conduct value analysis in order to determine how the functions of particular parts, materials, or services can be performed as well or better at a lower cost. Techniques such as brainstorming, hitchhiking, and leapfrogging are used during value analysis. It is a problem-solving tool.

Value chain
Activities in an organization are related to what is sometimes referred to as the value chain: inbound (receiving), operations (production or service), outbound (shipping), marketing, sales, and service. Value chain is related to supply chain.

Value stream
A value stream consists of the processes of creating, producing, and delivering a good or service to the market. For a good, the value stream encompasses the raw material supplier, the manufacture and assembly of the good, and the distribution network. For a service, the value stream consists of suppliers, support personnel and technology, the service "producer," and the distribution channel. The value stream may be controlled by a single business or a network of several businesses.

Value stream mapping
Value stream mapping is a technique of mapping the value stream for products and services and for vendors and suppliers.

Variant virus
A variant virus is a virus generated by modifying a known virus. Examples are modifications that add functionality or evade detection. The term "variant" is usually applied only when the modifications are minor in nature. An example would be changing the trigger date from Friday the 13th to Thursday the 12th.

Verification
Verification is the act of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether activities, processes, services, or documents conform to specified requirements.

Version configuration
A version refers to a change to a baseline configuration item that modifies its functional capabilities. As functional capabilities are added to, modified within, or deleted from a baseline configuration item, its version identifier changes.

Vertical analysis
Vertical analysis is: (1) an analysis that compares each item in a current statement with a total amount within the same statements; (2) a tool that converts financial statement numbers to percentages so that they are easy to understand and analyze.

Vertical market
A vertical market is a market in which the goods of one business are used as raw materials or components in the production or sale process of another business.

Vertical team
A vertical team is a formal team composed of a manager and his or her subordinates in the organization's formal chain of command.

Vertically integrate
To vertically integrate is to bring together more of the steps involved in producing a product in order to form a continuous chain owned by the same firm; it typically involves taking on activities that were previously in the external portion of the supply chain.

Virtual memory
Virtual memory is a technique by which the central process unit can use more memory than is available in a computer the main memory. Only active portions of a program are actually loaded into main memory.

Virtual organization
A virtual organization is an organization that (1) has few full-time employees and temporarily hires outside specialists who form teams to work on specific opportunities, then disband when objectives are met; (2) requires very little office space. Its employees telecommute, and services to customers are provided through telecommunications lines.

Virtual private network (VPN)
A VPN is a virtual network, built on top of existing physical networks, providing a secure communications tunnel for data and other information transmitted between networks. It uses a split tunneling method to route an organization's specific network traffic through the SSL-VPN tunnel, but other traffic uses the remote user's default gateway (gateway is a network interconnection).

Virtual reality
Virtual reality is a set of hardware and software that creates images, sounds, and possibly the sensation of touch that give the user the feeling of a real environment and experience. In advanced virtual reality systems, the user wears special goggles and gloves.

Virtual team
A virtual team is a team that uses advanced information and telecommunications technologies so that geographically distant members can collaborate on projects and reach common goals.

Virus
A virus is a self-replicating code segment attached to a host executable. (An executable is an abstraction for programs, command files, and other objects on a computer system that can be executed.) There are many types of viruses, including macro, worms, Trojan horse, resident, stealth, and polymorphic.

Visible pay inequity
Visible pay inequity between the expatriates and their local peers could demoralize the foreign subsidiary's staff.

Vision
A vision is: (1) an attractive, ideal future that is credible yet not readily attainable; (2) a statement that explains what the company wants to become and what it hopes to achieve.

Voluntary export restraint agreement
A voluntary export restraint agreement is an accord between countries to limit trade in specific goods. Such agreements are administered by the exporter and may or may not be formally negotiated.

Vroom-Jago model
The Vroom-Jago model is a model designed to help managers gauge the amount of subordinate participation in decision making.

Vulnerability
A vulnerability is a weakness or flaw that might be exploited to cause loss or harm.

Wait state
A wait state is the state in which a program is waiting for the completion of some event, such as an input/output operation.

Walk-through

A walk-through is a project management technique or procedure where the programmer, project team leader, functional users, system analyst, or manager review system requirements, design, and programming and test plans; design specifications and program code (1) to prevent errors in logic and misinterpretation of user requirements, design and program specifications and (2) to prevent omissions. It is a detective control.

In a system walk-through, for example, functional users and information systems staff together review the design or program specifications, program code, test plans, and test cases to detect omissions or errors and to eliminate misinterpretation of system or user requirements. System walk-throughs can also occur within and among colleagues in the information systems and system user departments. It costs less to correct omissions and errors in the early stages of system development than it does later. This technique can be applied to both system development and system maintenance.

Warm site

A warm site is a backup, alternate computer processing location that have the basic infrastructure of a cold site but also have sufficient computer and telecommunications equipment installed and available to operate the system at the site. However, the equipment is not loaded with the software or data required to operate the system. Warm sites are a part of information technology continuity planning.

Web bug

A Web bug is a Hypertext Markup Language (HTML) element, often in the form of image tags, that retrieves information from a remote Web site. While the image may not be visible to the user, the act of making the request can provide information about the user. Web bugs are often embedded in Web pages and HTML-enabled e-mail messages.

What-if analysis

What-if analysis is: (1) a trial-and-error approach to learning about the range of possible outputs for a model. Trial values are chosen for the model inputs (these are the what-ifs) and the value of the output(s) is computed; (2) an analysis that is conducted to test the degree to which one variable affects another. It is called sensitivity analysis.

Whistleblowing

Whistleblowing is the disclosure by an employee of illegal, immoral, or illegitimate practices by the organization.

White box testing

White box testing is a software test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. It focuses on the internal behavior of a system (program structure and logic) and uses the code itself to generate test cases. The degree of coverage is used as a measure of the completeness of the test cases and test effort. White box testing is performed at individual components level, such as program or module, but not at the entire system level. It is also known as detailed testing or logic testing and should be combined with black box testing for maximum benefit because neither one by itself does a thorough testing job. White box testing is structured testing since it focuses on structural analysis of a system. As such it is also called glass box testing, because the tester can see the inside of a system through a glass using test cases, test data, and program code.

White team

A white team is a neutral team of employees acting as referees and judges between a red team of mock attackers (offenders) and a blue team of actual defenders of their enterprise's use of

information systems. The white team establishes rules of engagement and performance metrics for security tests. The white team acts as observers during the red team activity because it has prior knowledge of unannounced red team activities and ensures that the scope of testing does not exceed a predefined threshold. Occasionally, the white team also performs incident response activities and addresses bot attacks on an emergency basis.

Whitelisting
Whitelisting is a method for controlling the installation of software by ensuring that all software is checked against a list approved by the organization. Whitelisting technology allows only known good applications and does not allow any new or unknown exploits to access a system. Whitelisting is a list of discrete entities, such as hosts or applications that are known to be benign.

Whitemail bribery
Whitemail bribery consists of payments made to induce an official in a foreign country who is in a position of power to give favorable treatment where such treatment is either illegal or not warranted on an efficiency or economic benefit scale.

Wide area network (WAN)
A WAN is a network concept to link business operations and computers used across geographical locations.

Work measurement
Work measurement is an industrial engineering program that applies some of the general principles of creative problem solving to the simplification of operations or procedures. It is a problem-solving tool.

Workbench
A workbench is a set of integrated software tools to make one's job productive and effective (e.g., programmer's workbench, analyst's workbench).

Workflow
Workflow is a graphic representation of the flow of work in a process and its related subprocesses, including specific activities, information dependencies, and the sequence of decisions and activities.

Working storage
Working storage is that portion of storage, usually computer main memory, reserved for the temporary results of operations.

Workstation
A workstation is a high-powered personal computer with multiple functions and connected to the host computer.

World-class (leading) organizations
World-class (leading) organizations are organizations that are recognized as the best for at least one critical business process and are held as models for other organizations.

World Intellectual Property Organization (WIPO)
WIPO is a specialized United Nations agency that promotes the protection of intellectual property throughout the world through cooperation among countries and ensures administrative cooperation among he intellectual property unions. WIPO administers a number of international agreements on intellectual property protection, including the Berne Convention for the Protection of Literary and Artistic Works and the Paris Convention for the Protection of Industrial Property.

World Trade Organization (WTO)
The WTO was created by the General Agreement on Tariffs and Trade as a formal organization through which member countries could administer the multilateral trading system.

Worm
A worm is a self-replicating, self-propagating, self-contained computer program that uses networking mechanisms to spread itself.

Worst-case scenario
A worst-case scenario is an analysis in which all of the input variables are set at their worst reasonably forecasted values.

Write
The term "write" refers to a fundamental operation that results only in the flow of information from a subject to an object.

Write access
Write access is permission to write an object.

Yield curve
A yield curve is a graph showing the relationship between yields and maturities of securities.

Zap
Zap is a powerful computer utility program that can alter data file and program contents, directly bypassing integrity and security controls (e.g., IBM's Superzap).

Zero-for-zero tariffs
Zero-for-zero tariffs is a concept introduced by the United States in March 1990, when it tabled a proposal advancing the elimination of tariffs in certain sectors through the request-offer approach.

Zombie
A zombie: (1) is a compromised Web server on which an attacker has placed programming code that, when triggered, will launch with other zombies, leading to a denial-of-service attack; (2) a program that is installed on one computer system with the intent of causing it to attack other computer systems in a chainlike manner.

Index