

Being Proactive With
Forensic Data Analysis

The Art of the Interview

Taking Fraud Off the Payroll

Internal Audit as Corporate
Conscience

A MATTER OF TRUST

Attention to detail and focused effort can help internal auditors build the relationships required to be perceived as valued advisers.





New Industry Report from TeamMate®

Wolters Kluwer Tax & Accounting


Who owns responsibility for the technology tools used by your audit department?

If you can't answer that, you may be falling behind. The latest research survey from TeamMate focuses on Technology Champions and the significant positive impact they can have on audit departments.

80% of those surveyed
view Technology
Champions as a key success
factor for their organization.

36% of CAEs see
Technology
Champions as a Key Strategic
Player in Audit Management.

View a copy of our latest report at:
TeamMateSolutions.com/TechChamp



How do you manage if you aren't measuring?

Find out how our market-leading global risk and internal audit practices look beyond assurance to provide business insights and help management anticipate risks.

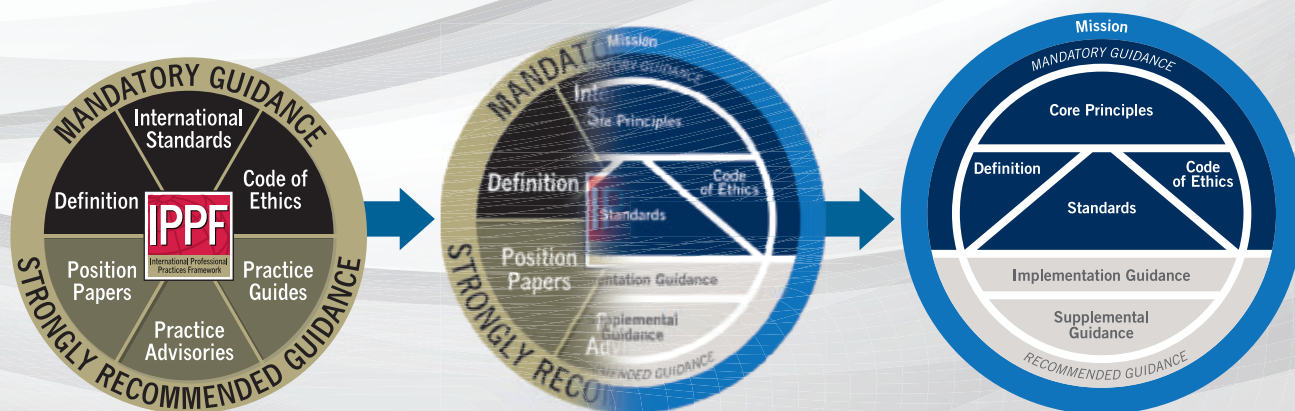
[ey.com/advisory](https://www.ey.com/advisory)



Be Part of the Change



International Professional
Practices Framework



The *Standards*: Evolving to Meet New Challenges

You play a critical role in evolving the *International Standards for the Professional Practice of Internal Auditing (Standards)* to meet the demands of the profession, its practitioners, and your stakeholders. To meet the challenges of today's business environment, there are proposed changes to the *Standards*.

This is **your opportunity** to weigh in and have an impact on these key changes, which include:

- Two new standards
- Alignment of the *Standards* to the Core Principles
- Key updates to existing standards

Access the proposed changes and provide your feedback Feb. 1 – April 30, 2016, at www.theiia.org/2016-Standards-Exposure.



 The Institute of
Internal Auditors



FEATURES

26 COVER A Matter of Trust Attention to detail and focused effort can help internal auditors build the relationships required to be perceived as valued advisers. **BY ARTHUR PIPER**

33 Proactive Fraud Analysis Integrating advanced forensic data analytics capabilities can help auditors mitigate fraud risks and demonstrate returns. **BY ADITYA MISRA AND VINCENT WALDEN**

38 Getting More From Interviews Instead of emphasizing formalities, internal auditors should approach each interview like a conversation. **BY J. MICHAEL JACKA**

45 On the Hunt for Payroll Fraud Taking a close look at payroll risks can enable internal auditors to help their organizations save money and identify wrongdoing. **BY CHRISTOPHER KELLY AND FRANS DEKLEPPER**

52 Guardians of Integrity Internal audit can provide

insight into corporate integrity and people-related risks. **BY MICHAEL BROZZETTI**

57 5 Steps to Agile Project Success The dynamic, fast-paced nature of Agile software development requires auditors to think differently about internal controls. **BY DAVID TILK**



DOWNLOAD the Ia app on the App Store and on Google Play!



New CBOK Reports Now Available

Download the latest reports from the Global Internal Audit Common Body of Knowledge® (CBOK®) Practitioner Study:

- GREAT Ways to Motivate Your Staff: Shaping an Audit Team That Adds Value and Inspires Business Improvement
- Interacting with Audit Committees: The Way Forward for Internal Audit
- Engaging Third Parties for Internal Audit Activities: Strategies for Successful Relationships

Your Donation Dollars at Work: CBOK reports are available free of charge.

Are internal auditors performing to stakeholders' expectations?



The first report, *Relationships and Risk: Insights from Stakeholders in North America*, from the CBOK Stakeholder Study is now available: www.theiia.org/cbok.

CBOK is administered by The IIA Research Foundation and funded by the William G. Bishop III, CIA, Memorial Fund. Learn more: www.theiia.org/cbok.

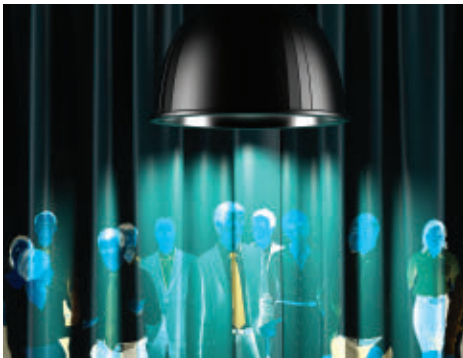


CBOK

The Global Internal Audit
Common Body of Knowledge



DEPARTMENTS



7 Editor's Note

9 Reader Forum

PRACTICES

11 Update IIA releases 2016 Pulse report; U.K. joint task force takes on bank fraud; and due diligence on third parties found lacking.

17 Back to Basics Effective controls remain key to fraud prevention.

22 Risk Watch Is internal audit relevant to collaborative risk management?

24 Fraud Findings "Mini frauds" are dangerous beyond their financial impact.

INSIGHTS

63 Governance Perspectives U.S. government updates guidance for federal auditors.

65 The Mind of Jacka "The Big Short" provides important risk management lessons.

66 Eye on Business Internal auditors continue to work to achieve "trusted adviser" status.

68 In My Opinion Government auditors need to support innovation.

ONLINE InternalAuditor.org



Emerging Bloggers Get fresh perspectives from the next generation of internal auditors. Visit our Emerging Leaders blog for discussions of risk trends, career issues, technology, and a host of other topics.

Cyber in Focus Internal auditors say cybersecurity is a rising priority on their increasingly technology-driven audit plans.

The Fake Ex-employer Fraud expert Art Stewart examines how people claiming to work for fictitious companies were able to receive state unemployment benefits.

How to Be Viewed as a Trusted Adviser Watch a panel discussion on how internal audit can change stakeholders' perceptions through increased reliability, credibility, and relationship building.



Find us on Facebook



Thank You for Making 2015 a Success!



Every contribution, no matter how modest, plays a part in what we can do to help invest in the internal audit profession.

Stay tuned for exciting news from The IIA Research Foundation as we evolve and grow, providing new resources to internal audit practitioners around the world.

To learn more, visit www.theiia.org/research.

Strategic Partners



Research Partners



Diamond Partners

(US\$25,000+)

IIA–Dallas Chapter
IIA–Houston Chapter
Protiviti
Robert Half

Platinum Partners

(US\$15,000 – \$24,999)

IIA–Chicago Chapter
IIA–Greater Boston Chapter
Wolters Kluwer

Gold Partners

(US\$5,000 – \$14,999)

Erich Schumann, CIA, CRMA
ExxonMobil Corporation
IIA–Detroit Chapter
IIA–Miami Chapter
IIA–Philadelphia Chapter
Lawrence J. Harrington,
CIA, QIAL, CRMA
Liberty Mutual Insurance
RSM
State Farm
Vanguard

Support The IIA Research Foundation.
Make Your Donation Today!
www.theiia.org/research



BUILDING A BETTER INTERNAL AUDITOR

I wonder if internal auditors ever get tired of hearing that they need to be “better, stronger, faster” — to steal a line from the ‘70s television show, “The Six Million Dollar Man” — or, if they are excited by the prospect of continually growing the profession, of becoming trusted, respected advisers to the organization’s leadership (see “A Matter of Trust” on page 26).

Although I’ve worked for and with internal auditors for 15 years, I am not an internal auditor. As someone looking in from the outside, I am continually impressed with what I see. You have to admire a profession that constantly strives to evolve, to expand its mandate to address the needs of its stakeholders, and to ensure the well-being of the organization.

However, achieving trusted adviser status is no easy feat, and internal audit seemingly has a ways to go. According to The IIA’s 2016 North American Pulse of Internal Audit research, one area internal auditors need to improve is interpersonal skills. An overwhelming majority of CAEs and directors who responded to the Pulse survey agree that soft skills, in general, are essential to the trusted adviser role. Yet when asked about proficiency, many respondents rated their average team member as only moderately proficient in most soft skills. For example, 49 percent rated their average team member as moderately proficient in organizing and expressing ideas clearly, and 9 percent rated the average team member as only slightly proficient at this skill.

In this issue, we take a look at one of the foundational soft skills of internal auditing—interviewing (see “Getting More From Interviews” on page 38). Author J. Michael Jacka says practitioners can do far more with interviews than just gather information, including leveraging the opportunity to gain insight into the way operations work and gauging attitudes about the organization and internal control environments.

Mastering soft skills is just one component of achieving trusted adviser status. In this month’s “Eye on Business” (page 66), Michael Rose of Grant Thornton and Eric Holt of KPMG discuss several other aspects and suggest what CAEs can do to ensure their auditors have the necessary skills and attributes to be considered trusted advisers as they advance within the organization.

There is little question internal auditors can achieve trusted adviser status. They just need the right tools. As “The Six Million Dollar Man’s” Oscar Goldman (sort of) says: We can rebuild internal audit. We have the technology. We can make it better than it was. Did I just date myself?

@AMillage on Twitter



CCSA®

CFSA®

CGAP®

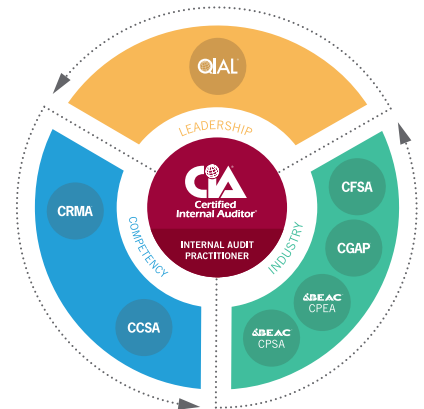
CRMA®



ABEAC

Drive Your Career Forward IIA Certifications and Qualifications

An IIA Professional Credential can take your career in the right direction, whether you're just starting down the audit path or taking your career to new elevations. Drive to new opportunity, with increased earning potential*, deeper knowledge, and enhanced credibility.



*According to The IIA's 2015 Internal Audit Compensation Study, the average salary of internal auditors who hold one or more certifications is 43 percent higher than that of peers with no certifications (based on U.S. responses).

Invest In Your Tomorrow, Today.
www.TheIIA.org/Certification



The Institute of Internal Auditors

Reader Forum

WE WANT TO HEAR FROM YOU! Let us know what you think of this issue. Reach us via email at editor@theiaa.org. Letters may be edited for clarity and length.



The IIA's 75th Anniversary Issue

Excito! Thanks for 75 years of sharing knowledge and raising the level of the profession. Congratulations.

ADRIA FERNANDEZ comments on LinkedIn.

Internal auditors from Bosnia and Herzegovina have learned a lot from you. Congratulations on contributing to the progress and enhancement of the profession.

NEDIM CUSTOVIĆ comments on LinkedIn.

Digital Disruption

After 15 years in the assurance profession, I made the switch to working in the digital space to begin to understand and experience this disruptive digital force first hand. A year and a half later, I

am firmly of the opinion that the question of relevance of audit functions will appear more frequently in the digital age. I have already begun to see it with a few large clients who are experimenting with digital operating models. Auditors from well-trained and seemingly forward-thinking teams simply have not been able to respond quickly enough to the pace of the massive digitally driven organizational shifts in strategy.

NAEEM SEEDAT comments on the *Chambers on the Profession* blog post, "Is Disruptive Innovation an 'Uber' Risk for Internal Audit?"

Retail Fail

Other examples could include some organizations' decisions to match or not match the prices of online retailers. In each case, the decision-makers have (one hopes) thought through the ramifications, both positive and negative, as well as both short- and long-term. In many cases, internal audit is not privy to these decisions and in others, comments from internal audit are unwelcome. Whichever way we look at this, internal audit can add relevance to its work by budgeting

executive time to connect with other parts of the business and understand the business strategy. Using data analytics could help cover the traditional risks and free up time to address other areas.

KRISH comments on the *Mind of Jacka* blog post, "Why Wal-Mart Will Fail."

Audit Report Omissions

It is common to omit personnel issues from audit reports, especially in light of human resources, legal, and other compliance and regulatory concerns. However, if potential problems were noted during the audit, they should have been discussed with the manager in question—couched in terms of risk, risk mitigation, and training rather than in terms of a failing management style. Auditors can document and track verbal recommendations just as easily as written ones, and while the report itself may not tell the whole story, Marks correctly points out that the report is not required by the *Standards* to be the sole communication channel.

RICHARD FOWLER comments on the *Marks on Governance* blog post, "What Do the Auditors Really Think?"

Ia
INTERNAL
AUDITOR

APRIL 2016
VOLUME LXXIII:II

EDITOR IN CHIEF

Anne Millage

MANAGING EDITOR

David Salierno

ASSOCIATE MANAGING EDITOR

Tim McCollum

SENIOR EDITOR

Shannon Steffee

ART DIRECTION

Yacinski Design, LLC

PRODUCTION MANAGER

Gretchen Gorfine

CONTRIBUTING EDITORS

Mark Brinkley, CIA, CFSa, CRMA
John Hall, CPA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Steve Mar, CFSa, CISA
James Roth, PhD, CIA, CCSA, CRMA
Paul J. Sobel, CIA, QIAL, CRMA
Laura Soileau, CIA, CRMA

EDITORIAL ADVISORY BOARD

Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, CGA, FCIS, FCMA
Mark Brinkley, CIA, CFSa, CRMA
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Daniel J. Clemens, CIA
David Coderre, CPM
Michael COX, FIA(ANZ), AT
Dominic Daher, JD, LL.M.
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Keith E. Johnson, CIA

Sandra Kasahara, CIA, CPA
Robert Kuling, CIA, CRMA, CQA
Michael Levy, CIA, CRMA, CISA, CISSP
Merek Lipson, CIA
Thomas Luccock, CIA, CPA
Michael Marinaccio, CIA
Norman Marks, CPA, CRMA
Alyssa G. Martin, CPA
Dennis McGuffie, CPA
Stephen Minder, CIA

Kenneth Mory, CIA, CPA, CISA, CRMA
Jack Murray, Jr., CBA, CRP
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Cathlynn Nigh, CRMA, CSSGB
Michael Plumly, CIA, CPA
Jeffrey Ridley, CIA, FCIS, FIIA
Marshall Romney, PhD, CPA, CFE
James Roth, PhD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debra Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PhD, CPA
Glenn Summers, PhD, CIA, CPA, CRMA
Sonia Thomas, CRMA
Stephen Tiley, CIA

Tom Tocash, CIA, CCSA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoor, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CFSa, CRMA

IIA PRESIDENT AND CEO
Richard F. Chambers, CIA,
QIAL, CGAP, CCSA, CRMA

IIA CHAIRMAN OF THE BOARD
Larry Harrington, CIA, QIAL,
CRMA, CPA



PUBLISHED BY THE
INSTITUTE OF INTERNAL
AUDITORS INC.

CONTACT INFORMATION

ADVERTISING
advertising@theiaa.org
+1-407-937-1109; fax +1-407-937-1101

SUBSCRIPTIONS, CHANGE OF ADDRESS, MISSING ISSUES
customerrelations@theiaa.org
+1-407-937-1111; fax +1-407-937-1101

EDITORIAL
David Salierno, david.salierno@theiaa.org
+1-407-937-1233; fax +1-407-937-1101

PERMISSIONS AND REPRINTS
editor@theiaa.org
+1-407-937-1232; fax +1-407-937-1101

WRITER'S GUIDELINES
InternalAuditor.org (click on "Writer's Guidelines")

Authorization to photocopy is granted to users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the current fee is paid directly to CCC, 222 Rosewood Dr., Danvers, MA 01923 USA; phone: +1-508-750-8400. *Internal Auditor* cannot accept responsibility for claims made by its advertisers, although staff would like to hear from readers who have concerns regarding advertisements that appear.



Data Designed for Development

Imagine What You'll GAIN Turning Your Information into Insights.

Do you want to know how your internal audit department measures up? The Global Audit Information Network® (GAIN®) Benchmarking Tool allows you to benchmark your internal audit department easily, affordably, and transparently. It lets you compare your audit department's size, experience, and other metrics against the averages of similar organizations in peer groups that YOU choose.

Find out how you compare with your peers with reliable data and metrics including:

- Performance measures.
- Organizational statistics.
- Department staffing and costs.
- Operational measures including audit life cycles.
- Risk assessment and audit planning information.
- Oversight including audit committee information.

No matter what your benchmarking needs are, the GAIN Benchmarking Tool has you covered. Your final report will benchmark your organization with participants in 17 industries, more than 100 sub-industries, and 42 countries, unlocking real answers to organizational questions.

Audit Executive Center® participants that complete and submit the questionnaire with their company data **receive a complimentary study.**

Get Started Today!
Visit www.theiia.org/goto/GAIN



 **The Institute of
Internal Auditors**

U.K. launches bank fraud task force... Vendor risk management lacking... Reforming global sports governance... DHS issues cyberthreat guidance.

Update



COMPLIANCE AND ETHICS HOT TOPICS

Compliance and ethics professionals list their top five concerns.

1
**CYBERSECURITY/
CYBERCRIME**

2
**SOCIAL MEDIA
COMPLIANCE RISKS**

3
**LEVERAGING COMPLIANCE
AND BUSINESS PRACTICES**

4
**CREATING/MAINTAINING
AN ETHICAL CULTURE**

5
**EFFECTIVE INTERNAL
INVESTIGATIONS**

Source: Society of Corporate Compliance and Ethics and Health Care Compliance Association, Compliance and Ethics Hot Topics for 2016

TIME TO SHIFT THE MIND-SET

Pulse report urges internal audit to focus on culture and cybersecurity response.

Following a year of scandal ranging from FIFA to Toshiba, most internal audit functions (58 percent) still aren't auditing the organizational culture qualities so vital to deterring such incidents, according to The IIA's 2016 North American Pulse of Internal Audit report. Among those functions, only 45 percent say internal audit is able to identify and assess organizational culture measures, compared to 80 percent of the respondents whose audit functions review culture.

"Lack of management and board support for internal audit's involvement in culture, and lack of internal audit's ability to

identify and measure organizational culture, are closely associated with internal auditors avoiding this risk," the Pulse report observes. The Pulse survey polled 486 CAEs and audit directors in North America.

Similarly, internal audit functions may not be ready to respond to today's sophisticated cyberattacks, with 52 percent saying their audit function lacks cybersecurity expertise. Despite a growing expert consensus that such incidents are inevitable, 53 percent consider prevention to be the most effective method of addressing cyberattacks. "In the face of a cyberattack, addressing business continuity and reputational risk are paramount,"

FOR THE LATEST AUDIT-RELATED HEADLINES follow us on Twitter @laMag_IIA



THE INSTITUTE OF INTERNAL AUDITORS
**INTERNATIONAL
 CONFERENCE**
 NEW YORK, NY, USA / JULY 17-20, 2016



The IIA's International Conference – the premier training and networking event for internal audit professionals worldwide.

Register today and enjoy The IIA's 75th anniversary celebration with long-time peers and new connections alike at once-in-a-lifetime networking events.

100+ Speakers From Around the Globe
70+ Sessions in 10 Educational Tracks
2,000+ Attendees From 100+ Countries

Inspire your future with educational sessions focused on IT, leadership, public sector, emerging practices, fraud, risk and exposure, financial services, The IIA's CIA Learning System® Review, a full Spanish track, and more.

Confirmed Keynote Speakers



Olivia Kirtley
*President
 International Federation
 of Accountants;
 Audit Committee Chair:
 Papa John's International,
 ResCare Inc., US Bancorp,
 USA*



Richard Quest
*CNN International
 Business Correspondent
 and Host of Quest
 Means Business*

Join us in New York and enjoy the city's energy, culture, and attractions — plus the Conference's dynamic and diverse program.

Register now at ic.globaliia.org.



says IIA President and CEO Richard Chambers. “Yet few organizations are taking time to think beyond prevention.”

Audit leaders are concerned about the quality of data stored on their organizations’ systems. “The power of data to inform decisions comes with the potential to misdirect organizations,” the report points out. “Problems can arise from data collection, data analysis, and decisions made from the data.” Yet nearly half of respondents (47 percent)

say internal audit has little involvement in evaluating the quality of such data.

In addition to enhancing their data analytics capabilities to better assess data quality, internal auditors also need to boost their interpersonal skills if they hope to become trusted advisers, the report points out. Although the vast majority of audit leaders say such skills are essential, they rate their team members as just moderately proficient in specific skills on average. —**T. MCCOLLUM**

U.K. TASK FORCE TAKES ON BANK FRAUD

Government and lenders pool resources to fight fraudsters.

A recently announced U.K. government initiative will combine efforts from the nation’s banks, police, and government officials to fight fraud. The Joint Fraud Taskforce, led by the U.K.’s Home Office, aims to increase coordination among participating groups to address the country’s growing fraud levels.

The task force includes representatives from the country’s four largest banks—Barclays, HSBC, Lloyds Banking Group, and Royal Bank of Scotland—as well as smaller lenders. Participating institutions are committing to identify fraud victims more quickly by training staff in bank branches and increasing customer awareness.



Initial priorities for the task force include finding ways to better understand the threat of fraud and to spot intelligence gaps. The group also seeks a more coordinated approach to organized crime, including development of a 10 most-wanted list of U.K. fraudsters. Moreover, it will look to remove weak links in banking processes.

The group intends to build on existing efforts across financial services and law enforcement, including the Dedicated Card and Payments Crime Unit, where police and industry investigators collaborate to disrupt fraudsters. It also will draw on the work of the National Fraud Intelligence Bureau, operated by the City of London Police. —**D. SALIERNO**



49%

OF BOARD MEMBERS SAY THEIR ORGANIZATION HAS THE CAPABILITIES OR PROCESSES IN PLACE TO HANDLE A CRISIS WITH THE BEST POSSIBLE OUTCOME.

50%

SAY THEIR ORGANIZATION HAS EVALUATED KEY CRISIS SCENARIOS AND JUST

43%

HAVE EVALUATED WORST-CASE SCENARIOS.

“Board members should discuss with management to ensure there is a sound and common understanding of risks that can leave an organization vulnerable to crisis,” says Peter Dent, leader of Deloitte’s Global Center for Crisis Management.

Source: Deloitte Touche Tohmatsu Ltd., A Crisis of Confidence

RISKY VENDORS

Third-party due diligence and risk management programs found lacking.

Despite recent third-party compliance failures, 32 percent of respondents to a NAVEX Global survey don’t scrutinize outside vendors before doing business with

them. Nearly half (46 percent) lack a dedicated budget for third-party risk management, and 11 percent don’t know how many third parties their organization works with, according to the 2015

Ethics & Compliance Third Party Risk Management Benchmark Report.

Such findings appear to contradict the 90 percent of respondents who cited “protect our organization from risk and damage” as the top objective of their third-party risk management program, according to the global survey of more than

DEMONSTRATE YOUR LEADERSHIP EXCELLENCE



Qualification in
Internal Audit Leadership®

You're successful, respected, and committed.
What does it take to get to the next level?

The QIAL identifies, assesses, and develops core skills linked to audit leadership success. It caters to CIAs and CAEs who are already strong performers and have the potential for greater leadership.

Start your leadership journey **TODAY** at globaliia.org/QIAL.



VISIT <http://bit.ly/1pqTcfF> to read an extended interview with Gareth Sweeney.

300 ethics and compliance professionals. Respondents' top concern is bribery and corruption (39 percent), which reflects the increased regulatory enforcement and prosecutions of laws such as the U.S. Foreign Corrupt Practices Act and U.K. Bribery Act. Many of these cases carry large fines and penalties, along with civil and criminal sanctions, the report notes. Fraud (23 percent) and conflicts of interest (19 percent) round out the top three concerns.

Although organizations can pinpoint which third-party failures to fear, they lack the programs to manage those risks, says Randy Stephens, vice president, advisory services at NAVEX and author of the report. "There are signs that organizations—often at the behest of their boards—are ramping up third-party due diligence and risk management programs," he observes. "However, many are struggling to create scalable, solid, defensible third-party risk management programs." Stephens adds that although it's reassuring that almost two-thirds of respondents' organizations are scrutinizing third parties before working with them, many times, the initial evaluation is not robust enough. "Strong third-party risk practices need to be supported by a culture of compliance, which is best established by the right tone from top and middle managers," he says. —**S. STEFFEE**

SPORTS REFORM ON THE HORIZON

International sports organizations (ISOs) can learn from corporate governance best practices, says Gareth Sweeney, head of Transparency International's Corruption in Sport Initiative.



What will be the impact of the new FIFA reforms? The general framework could go a long way toward addressing fundamental deficiencies in the organization. Many important elements are there, including term limits, compensation and asset disclosures, the creation of a new council with a limited managerial role, a fully independent audit and compliance committee, and an independent chair of the development committee. We still have to see what FIFA really means by "independent" and what eligibility criteria will be applied to new positions.

What lessons can ISOs draw from governance reform in other sectors? In many ways the insularity of sports governance is unique, but one key recommendation Transparency International has made to ISOs since 2011—which FIFA has continued to overlook—is the need for independent, nonexecutive directors at the board level. The value of external expertise and oversight is well-established in corporate governance, yet it is something sports organizations continue to skirt around. There is still a huge amount to be done in changing the culture of ISOs for members to realize that increased accountability is ultimately in their sport's best interest.

THE POWER OF SHARING

The DHS issues guidelines for exchanging cyberthreat information.

The U.S. Department of Homeland Security (DHS) recently issued guidelines and procedures mandated by the information-sharing provisions of the Cybersecurity Act of 2015. In addition to spelling out how U.S. organizations may monitor and defend their computer networks, the law permits private-sector organizations and the federal government to share cyberthreat information.

"These guidelines provide federal agencies and the private sector with a clear understanding of how to share cyberthreat indicators with DHS' National Cybersecurity and Communications Integration Center (NCCIC) and how the NCCIC will share and use that information," DHS Secretary Jeh Johnson says.

To facilitate information-sharing, Johnson says the NCCIC has enhanced its

Automated Indicator Sharing system to meet Cybersecurity Act requirements. Moreover, the DHS is enlisting companies to help establish a technical infrastructure for sharing and receiving cyberthreat indicators in real time.

To ensure data privacy as required by the new law, the guidelines detail how companies must remove personal information before sharing threat indicators and how the DHS will conduct privacy reviews. —**N. LICOURT**





Audit Management Software

| | 2006 | 2015 |
|------------------------------------|----------|---------------|
| CUSTOMERS | 25 users | 25,000+ users |
| VERSION | 2.0 | 10.0 |
| REPLACEMENT OF TRADITIONAL SYSTEMS | 0 | 70+ countries |
| OUTBOUND SALES CALLS | 0 | 0 |

How has MKinsight™ become
the fastest growing
Audit Management Software
worldwide without making
a single outbound sales call?

+1 847 418 3898
www.mkinsight.com

Trusted by Companies, Governments and Individuals Worldwide.

Back to Basics

BY LOUISE HENRY EDITED BY JAMES ROTH + LAURA SOILEAU

FRAUD PREVENTION

An effective control environment can deter or minimize the occurrence of fraudulent activities.

Even in a rapidly changing business environment with emerging technologies and constant challenges, at the core of every organization is its employees—those carrying out operations, executives, administrative personnel, and even the board. Employees are faced with an increasing pressure to meet the bottom line at work and at home, and they can be exposed to a variety of ethical dilemmas. These dilemmas can tempt employees to commit fraud against their employer.

The cost of occupational fraud can be minimized with fraud prevention. Depending on the size and complexity of an organization, internal audit can be called on to recommend improvements or evaluate an organization's controls and commitment to fraud prevention. An organization's internal controls are not always specifically designed to prevent fraud; however,

often there are fraud prevention components inherent in internal controls related to the control environment, segregation of duties, and monitoring activities.

Control Environment

The control environment is one of the interrelated components of internal control, and it is vital in establishing an effective fraud-prevention culture within an organization. A visible commitment to fraud prevention can exhibit to employees the importance of anti-fraud measures to the organization. Control activities related to fraud prevention can be evident in the hiring, onboarding, and training of employees, as well as the organization's policies and procedures.

During the hiring process, companies may conduct background checks, validate references, or confirm certifications. Certain fields or industries may require background checks, which

can serve as a first point of communication regarding an organization's tolerance of fraudulent activity.

The introduction to the organization's mission and values typically occurs during the onboarding process. This can be an opportune time to distribute and explain the code of conduct, code of ethics, or a separate fraud policy. Taking time to discuss the firm's policies and procedures thoroughly can be an effective measure in fraud prevention. For example, organizations subject to bid requirements should maintain sufficient documentation to support compliance with established protocols in place. Policies and procedures should be clearly defined, published, readily available, and required to be read and acknowledged annually by employees to correspond with terms of employment.

Fraud-related training can reinforce the importance of anti-fraud, waste, and abuse measures to the

SEND BACK TO BASICS ARTICLE IDEAS to Laura Soileau at Isoileau@pncpa.com

PREPARE TO PASS THE CIA[®] EXAM

NEW for 2016! **StudyPLUS**

When you're in the home stretch and want a final confidence boost for the CIA exam, The IIA's StudyPLUS is your competitive edge. The IIA's CIA Learning System[®] provides everything you need to prepare for the Certified Internal Auditor[®] (CIA) exam, PLUS, with these exciting new tools and tips you will feel even more in control on exam day.



Take your exam day confidence over-the-top with The IIA's CIA Learning System.

Easily access StudyPLUS on your computer, tablet, or mobile device wherever you are, day or night:

NEW! ✓ CIA Exam Tips & Techniques Video

NEW! ✓ Bonus Printable Practice Questions

NEW! ✓ Guide to Knowing When You're Prepared

NEW! ✓ Guide to CIA Exam Scoring

NEW! ✓ CIA Question Analysis Grid

NEW! ✓ Study Tips from Successful Candidates

For more information or to create your free study plan, visit www.LearnCIA.com/plus.



 The Institute of
Internal Auditors



TO COMMENT on this article,
EMAIL the author at louise.henry@theiaa.org

organization. To be effective, training that promotes fraud prevention should be tailored to the role and duties of the individual employee. Mandatory, continuous training for employees who progress within an organization can be implemented based on individual job responsibilities and within a department's specific function. This can equip employees with the skills to detect fraud, and also educate employees about what to do when fraud is suspected.

Companies may opt to use hotlines for fraud reporting. Depending on available resources, an organization's fraud reporting hotline may be third-party managed, in-house, or a combination of both. Information regarding the fraud reporting hotline should be communicated during training, readily available, and publicly displayed in common areas so it is visible to all employees. To build the trust of employees in the

Segregation of duties should occur at all levels of an organization.

fraud-reporting process, disseminated materials should contain information regarding how hotline tips are evaluated, and what level of anonymity and confidentiality can be assured for the tip-reporting employee.

Segregation of Duties

The organization should provide employees with the authority to carry out their duties, but no single employee should have the ability to create, execute, and monitor activities within a business function. For example, in payroll processing, there should be separation between the ability to approve payroll, write and sign checks, receive bank statements, and reconcile those bank statements. In this instance, an accountant or other financial personnel could approve payroll, write checks, and reconcile bank statements; whereas an executive director could sign checks, receive and open bank statements, and review bank reconciliations.

The size of an organization can create complexities related to segregation of duties. Small organizations can experience challenges because of staff size limits. Careful consideration should be made so that no single employee has complete control over all aspects of a process or function. However, large organizations can experience distinct challenges because of the potential overlap of job duties among multiple departments, which can require a more concerted effort to determine whether job responsibilities are adequately segregated.

Regardless of the size of an organization, controls should be designed and implemented so they cannot be overridden

without appropriate authority. Insufficient safeguards and consideration for employee responsibilities can lead to collusion. Segregation of duties should occur at all levels of an organization and be relevant to each specific function.

Comprehensive Monitoring


Monitoring implemented controls not only provides oversight, but it also can gauge compliance with established policies and determine whether controls are operating as intended. For example, controls established to segregate employee duties will be ineffective if those employees disregard controls in place. Ineffective controls can create the opportunity for an employee to perpetrate fraud. Monitoring should occur at all levels of an organization and not be limited to day-to-day operations.

Before establishing monitoring procedures, those responsible for monitoring activities should perform a fraud-risk assessment. Analytics are often used, but there are additional resources for an organization to consider. Employees are a valuable resource because they are close to the operations responsible for achieving

components of the organization's goals. Those performing the fraud-risk assessment should use the skills and knowledge of employees to strengthen monitoring activities. Employees can provide insight on how someone might circumvent current controls, which in turn can help an organization strengthen controls designed to prevent the occurrence of fraud. The involvement of employees in the fraud-risk assessment process provides them with increased fraud awareness. They can become more knowledgeable of fraud terms and schemes such as asset misappropriation and procurement fraud. Lastly, involvement of employees fosters continuous training and reinforces the organization's established policies and procedures.

Publicizing monitoring activities within the organization can help deter employees from committing fraud because they realize the likelihood of detection is increased. Monitoring can serve as a preventive measure within the organization and can also minimize the duration of fraudulent activity.

It Can Happen Here

As businesses grow or are redefined, fraud often presents itself unpredictably. Organizations that ignore the occurrence of fraud or maintain the "it can't happen here" mind-set may find themselves dealing with increasing fraud-related costs. Carefully designed and monitored preventive measures are crucial in the fight against fraud. 

LOUISE HENRY, CIA, CFE, is a consulting manager at *Postlethwaite & Netterville* in New Orleans.



THE INSTITUTE OF INTERNAL AUDITORS
**INTERNATIONAL
CONFERENCE**
NEW YORK, NY, USA / JULY 17-20, 2016



The IIA's International Conference – the premier training and networking event for internal audit professionals worldwide.

Register today and enjoy The IIA's 75th anniversary celebration with long-time peers and new connections alike at once-in-a-lifetime networking events.

100+

Speakers From Around the Globe

70+

Sessions in 10 Educational Tracks

2,000+

Attendees From 100+ Countries



Register now at ic.globaliia.org.
Special discounts for groups of 10 or more.



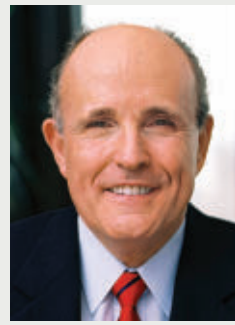
Inspire your future with educational sessions focused on IT, leadership, public sector, emerging practices, fraud, risk and exposure, financial services, The IIA's CIA Learning System® Review, a full Spanish track, and more.

Confirmed Keynote Speakers



Julia Gillard
Former Prime Minister of Australia

Time magazine's "100 Most Influential People in the World" and *Forbes*' "World's Most Powerful Women"



Rudolph J. Giuliani
Former Mayor of New York City

Topic: Principled Leadership in the Face of Change and Crisis

Join us in New York and enjoy the city's energy, culture, and attractions — plus the Conference's dynamic and diverse program.



*Early savings end March 15, 2016.

2015-1776

Risk Watch

BY DAN CLAYTON EDITED BY PAUL SOBEL

COLLABORATIVE RISK MANAGEMENT

As organizations consolidate their risk processes, internal audit may not be able to continue to stand alone.

Over the past decade, nothing has changed as rapidly as how people access and use information. Can you imagine buying a standalone GPS for your car today? Not likely, because every smartphone has that technology, and it is likely receiving real-time updates. Neither would people dial “411” for information when they could simply find it online or through an app.

Internal auditors provide information, too. However, are they applying old frameworks and producing individual reports, while management and boards are investing in technology that is capable of integrating most risks and issues across the business?

Much of the rapid change in risk management over the past decade has come from the internal audit profession’s advocacy of more formal risk governance and management. As advisers to the board and management,

internal auditors may have been instrumental in the creation of the first enterprise risk management function or risk committee, but they should also be the ones to advocate tearing them down if they are not working.

Today’s risk management discussion is less about a top-level function and more about risk collaboration and organizing risks and issues. Auditors need to be part of the change by understanding risk management’s potential future and planning to fill an appropriate, collaborative, and valued role.

Anticipate the Future

Internal auditors who have been in an audit committee meeting have likely faced questions like, “How does your risk assessment differ from the compliance risk assessment?” or “Are these IT issues part of the information security briefing?” They also may have heard members say, “Can’t we put this all together in one list?”

In short, as management owns risk management and the board starts to digest the results, they are looking for efficiency, comparability, and simplicity. It doesn’t always matter to them where the risk or issue came from.

In the future, organizations may establish one place where all risks and issues from all lines of defense are aggregated and digested for reporting purposes. This doesn’t necessarily mean all risk functions will merge—it means risks and issues will be organized by taxonomy (a shared set of terms) and within a common technology.

Such technologies already exist. These governance, risk management, and compliance (GRC) tools aspire to principles advocated by the Open Compliance and Ethics Group for bringing good governance, risk management, and compliance together into efficient systems, rather than redundant or dysfunctional

SEND RISK WATCH ARTICLE IDEAS to Paul Sobel at paul.sobel@gapac.com



TO COMMENT on this article,
EMAIL the author at dan.clayton@theia.org

processes. Early GRC applications were mainly successful in compliance, yet they now have collaborative potential. Although many GRC vendors have a shared risk register feature across compliance, legal, and other risk management modules, most of their audit modules are siloed in some respect, such as maintaining a separate risk universe. Integrating internal audit's broad risk perspectives, with risk detail from compliance, information security, and other risk functions can be done effectively without losing their uniqueness. The combined efforts would not only meet management and board needs, they would improve internal audit's processes and products, as well.

Internal audit would gain efficiencies from having a shared risk register to draw from at the beginning of its risk assessment process, or a shared list of ongoing concerns and follow-up status (monitored by the identifying risk function) for each area of the organization. Similarly, linking all this detail to either a strategic initiative or operational objective "at risk" could improve management's development and control over critical objectives, echoing the adage "knowledge is power."

Know Thyself

To engage in a future where risk and issues are consolidated, internal auditors must first have a strong sense of who they are. More than ever, the profession comprises individuals of

Auditors should be open to other ideas on organizing and mitigating risk.

varied backgrounds. However, at the heart of the internal audit profession's history, models, and skills is a risk perspective of mitigation and control.

Internal auditors' core skills can become a weakness if they dominate the implementation of enterprise risk processes and risk registers. Auditors are used to building dedicated processes to serve their own assessment and reporting needs, rather than defining how risk may be integrated into existing management oversight and operations development functions. As a result, auditors' dedicated risk processes too often are perceived by management as redundant.

Auditors should be open to other ideas on organizing and mitigating risk. Can management think of a better way to integrate risk considerations and outputs in existing processes? Probably. Yet, no one within the organization has a role with a scope broad enough to cover the whole organization. This puts internal auditors in a great position to be


a risk adviser and an engine for professional risk and issue management collaboration. However, to be effective, auditors have to understand the existing management processes, structure, and technologies by becoming students of how strategies and operations are defined, developed, and deployed.

For example, internal auditors often talk about aligning risk with strategies. However, from management's perspective, a strategic plan may be a short document with a handful of initiatives reflecting a desired destination. In reality, the organization's operating plan is what describes the complexity of the business through organizational charts, roles and responsibilities, purpose statements, and delegated authority. It is more appropriate to align risk with the operational objective affected, which would enable internal audit's discussions to easily zoom in or out on the organization's objectives and risks. Auditors can't do this without understanding the organization.

Know What Stakeholders Need

The more internal auditors can integrate their work into developing risk management processes, the more information management and the board will have to make good decisions. Risk and issue data integration means internal auditors need to understand management, which looks at objectives and operations in terms of "development" and "stages of maturity." Auditors need to be capable of seeing where the organization is as it progresses toward its objectives. Their risk management advice should focus on helping management discover threats to objectives in language executives can follow. Is it a top operational objective at risk, or a sub-objective? Are auditors

talking about an oversight risk or a risk related to aligning the right people, processes, and technology? As auditors' risk and issue information integrates with other risk-related functions, the quality of risk reporting to management and the board can improve along with the value of internal audit's services.

Internal auditors help organizations reach their objectives by advising them on governance, risk management, and control. If auditors are too comfortable producing their tried and true, process control audit reports, they will miss a significant opportunity to participate in the future of risk management and good governance. It will come, but it may not come on internal audit's terms. 

DAN CLAYTON, CIA, CPA, CKM, is director of Strategy and Knowledge Management with the System Audit Office at The University of Texas System in Austin.

Fraud Findings

BY JAMES SCOTT EDITED BY JOHN HALL

THE TICKING ETHICAL TIME BOMB

The financial loss from theft was secondary to the effect on company culture.

Axel Co. was a manufacturing company that operated a large industrial complex. Because of the size of the plant and its related infrastructure, the company had a significant ongoing investment in maintenance and repair, especially in maintenance supplies. Axel spent millions each year on steel, cable, and similar materials—and now some of it was going missing.

The primary supplies were maintained in a warehouse, where they were protected by physical access controls. But leftover supplies—for example, when a job used only 900 feet of a 1,000-foot roll of coaxial cable—were left in a less secure, open area called “the Yard.” Controls over the Yard were minimal because the supplies needed to be quickly and easily accessed for small maintenance jobs.

This system appeared to be working efficiently,

until a regular audit of the maintenance function revealed that items were disappearing from the Yard without explanation. Based on audit testing, the auditor, Stuart Wathen, estimated that annual losses would be in the tens of thousands of dollars if it wasn’t stopped.

At first, Wathen assumed that Axel maintenance staff was using the supplies and that the jobs simply had not been entered into the maintenance log. This proved not to be the case. He then hypothesized that local college students might have taken the items, possibly as a fraternity initiation prank. This, too, turned out to be incorrect. Finally, Wathen set up a concealed surveillance camera to find out what was really going on. The results were surprising and disturbing.

Many of Axel’s employees were skilled handymen and carpenters, with the

ability to build their own garages and cottages. As it turned out, many of these employees were stealing supplies from the Yard to take home for their own projects, and ignoring the posted signs, which clearly stated that these items were not trash but valuable company property.

On further investigation, the problem got even worse. Not only were the employees unrepentant about stealing company property, but they also bragged to co-workers about the creative ways they snuck their loot back to their cars and trucks past the security guards at the front gate. One worker even liked to boast that the Yard had built his entire garage—he had not paid for even a single nail or foot of wire. And the worst part was the other employees encouraged and supported this behavior, comparing the thieves to modern-day Robin Hoods.

SEND FRAUD FINDINGS ARTICLE IDEAS to John Hall at john@johnhallspeaker.com



TO COMMENT on this article,
EMAIL the author at james.scott@theia.org

The company was faced with a dilemma. The financial loss, while real, was clearly secondary to the effect on company culture. Axel was aware of “slippery slope” research, which shows that small frauds frequently lead to larger ones. Having a workforce that celebrated thieves as heroes was a recipe for future disaster. But their alternatives were limited. Shutting down the Yard, and moving the scraps to the warehouse, would be inefficient (that was why the Yard was created in the first place) and would do nothing to address the ethical conundrum. Prosecuting the employees for theft would be difficult and—in Axel’s highly unionized environment—would generate more ill will toward management than the issue was worth. Installing security cameras and stationing full-time security guards at the Yard would not be cost-effective. Telling the employees that they could take whatever they liked from the Yard was another option, but one that could lead to employees taking everything whether they needed it or not—and potentially to fights between employees about who could take which items.

In the end, Axel came up with a simple, elegant solution. The company put price tags on each item in the Yard, at prices substantially lower than market, and installed an

Sometimes the most obvious issue is not the more important one.

honor charity box for the United Way. It put up signs telling employees they could take whatever they wanted, but they were asked to put the appropriate sum into the United Way box. The contents of the box would then be emptied and given to the charity on a regular basis. There would be no guards or security cameras.

Axel also added a sign that read, “Total contributed to the United Way so far = \$xxx.” Behavioral psychology studies have found that people tend to behave more positively when they are reminded of their membership in a positive group.

Axel’s innovation was a great success. Employees who would (tacitly or otherwise) support fellow employees who stole from the company were far less willing to condone stealing from the United Way. The bragging about unethical behavior stopped almost immediately, and employees began to take pride in the ever-mounting total contribution to the charity. In many cases, employees even contributed amounts in excess of the price tags on the goods they took and started bragging about that. A ticking ethical

time bomb had been transformed into a source of strong ethical reinforcement.

Lessons Learned

- Organizations should be aware of situations that permit—or even encourage—“mini frauds,” as considerable research suggests small frauds lead to larger frauds. Such situations can be dangerous beyond their own financial impact.
- It is often easy for otherwise ethical employees to justify taking financial advantage of their employer (the rationalization side of the Fraud Triangle). It is accordingly dangerous to assume that other employees will discourage such behavior, at least on a small scale.
- In the past, many companies attempted to establish an ethical culture by reinforcing penalties for undesired behavior. But it is sometimes more powerful to establish identity in an ethical group as a proactive way to reinforce a positive image.
- Sometimes the most obvious issue is not the more important one. In this case, if Axel had focused on safeguarding the material in the Yard, it would have missed the more important ethical concern. The solution Axel adopted cost them money, but the ethical reinforcement was of far greater value.
 - The conventional response to an uncovered fraud is to increase controls. This is often valid, but an auditor should first examine the circumstances that encourage the fraud to see if the controls are unrealistic or inappropriate. Policies and limitations should not just be knee-jerk reactions that all but guarantee noncompliance.
- Controls can be more effective when external parties are involved. If the donation box had just said “money for charity,” it is possible that Axel employees would have been less motivated to pay for Yard materials. But by explicitly designating the donations for the United Way—a charity with whose good work the employees were all familiar—Axel made it even harder for employees to continue to justify the thefts.
- It is important for a company to monitor its ethical culture. In this case, Wathen heard about the bragging from friends who worked in the complex. Had he not found out about it, or if he had ignored it, Axel could have missed this ethical issue.

JAMES SCOTT, CIA, CPA, CPA-CA, CRMA, is a principal at *Ascot Solutions Inc. in Toronto.*

A MATTER OF TRU

Attention to detail and focused effort can help internal auditors build the relationships required to be perceived as valued advisers.

A

s boards and audit committees are being charged with more risk management and internal control oversight within their businesses, they have increasingly turned to internal audit for help. In addition to providing assurance on organizations' core functions, auditors have been involved in advising boards on key strategic initiatives—with some enjoying the status of trusted adviser. That is both a recognition that traditional audit work is not enough on its own to help the business execute its strategy in the face of emerging risks, and a realization that internal auditors can do more. In fact, just 16 percent of CAEs, senior management, and board members surveyed in PricewaterhouseCoopers' 2016 State

ST

Arthur Piper

of the Internal Audit Profession study say internal audit is currently providing trusted adviser services.

Trusted adviser can mean different things to different auditors, so some clarity is needed on what the role entails. But demand for a different level of service is evident. Not all auditors are comfortable with this shift, and many board members have either not experienced this level of service or are unaware that it exists.

“Checklists and audit plans often dominate the time and focus of internal audit teams,” says Olivia Kirtley, president of the International Federation of Accountants and audit committee chair for Papa John’s International, ResCare Inc., and US Bancorp. Moving away from that approach involves investment by the board and the audit department to free up some time from everyday audit work. “Internal auditors must be encouraged and have permission to devote time to innovation,

gaining understanding of evolving challenges, and initiating conversations with people throughout the business regularly about their issues and challenges. Importantly, this applies equally to business areas not under a current audit,” she says.

SHIFT IN THINKING

Mark Carawan, chief auditor for Citigroup in New York, and current president of the Chartered Institute of Internal Auditors, says taking on the trusted adviser role entails a large shift in the working relationship between the CAE and the board. “Being the trusted adviser to the board means that the internal auditor needs to be in a position where she or he can, at any point, initiate contact with the designated board member to raise something.”

Instead of contact being confined to communicating audit findings during formal meetings, the CAE should be free to talk about emerging issues that the board should be aware of as soon as those issues arise. “The internal auditor is helping inform the board member about current and emerging risk, candidly giving information on how the independent internal auditor is proceeding, how management is addressing that risk, he says. “Also, within the trusted part comes the ability to benchmark and give a qualitative view of positioning within the marketplace,” he explains.

Carawan says auditors build trust when their advice demonstrates external awareness of what competitors, regulators, and others are doing. “That’s really valuable to board members and, if you can provide that, they’re ready to pick up the phone the next time because they say ‘OK, last time

BUSINESS ACUMEN



A MATTER OF TRUST

I spoke to him, I got a really good heads up about something coming down the pipeline.”

That trust, when in place, cuts both ways. Carawan says when the audit committee chair has trust in the CAE, he or she is more likely to share information confidentially that will help the function match its work with the organization’s strategic goals. That communication is essential for audit planning and business intelligence because it forewarns the CAE about product launches, withdrawals, downsizing, outsourcing, and other strategic decisions that have a major impact on the business and the relevance of internal audit’s work.

Internal audit can often be forgotten if it is not part of the core team, because it is less visible than those functions that meet and talk regularly.

PART OF THE TEAM

Mark Salamasick, executive director of audit at the University of Texas System (UT System) Austin, has been promoting what he calls a consulting approach to internal auditing since the 1980s. He was pleased when The IIA revised the definition of *internal auditing* to include the term *consulting* in 1999 and less than thrilled when the U.S. Sarbanes-Oxley Act of 2002 gave audit a hugely onerous compliance role. “That basically set us back 13 to 14 years,” he says.

For him, being a trusted adviser means being accepted as part of the management team. In the UT System, which comprises 14 bodies, the organization’s chief internal auditor, J. Michael Peppers, is part of the chancellor’s executive management team that sets the strategic direction of the organization. Salamasick says internal audit can often be forgotten if it is not part of the core team, because it is less visible than those functions that meet and talk regularly about strategy and upcoming projects. Part of the problem, he says, is that more auditors are working remotely, using IT as an efficiency measure, but sacrificing the face time that builds up rapport and trust. Other internal auditors just do not see themselves in that role and stick more to traditional compliance work. Salamasick says they are mistaken.

“As soon as you have relationships built with management and you are integrated into the team, your decisions help

improve every level of the three lines of defense,” he says. It helps internal audit have a presence on major initiatives and projects and begin to move from historical auditing to looking forward and advising the organization on its strategic goals. It helps internal audit become change agents in the business.

RELATIONSHIP SKILLS



COMMUNICATION

62% of CAEs expect the role of internal audit to become that of a more **proactive** trusted adviser within the next five years, according to PwC's 2016 State of the Internal Audit Profession study.



TO COMMENT
on this article,
EMAIL the
author at arthur.piper@theiia.org

Kirtley also sees relationship building as critical. “Initiating conversations with business lines to truly understand the business and their current challenge is an area that can bring great value,” she says. “These conversations help align internal audit as a valued business partner that will not only call failures and successes on the current control and risk environment, but will also help business lines better anticipate and prepare for any troubled waters that might lie ahead.”

MAINTAINING INDEPENDENCE

Critics would argue that having too close a relationship with management threatens the internal audit department's independence. Maintaining independence entails ensuring the board knows that internal audit is serving the best interests of the organization—something that is increasingly difficult in a heavily regulated world. “As demands from regulators increase, internal audit needs to balance independence, being a trusted adviser to audit committees and executive management, and being an extension of the regulator where they can rely on the function,” says Paulette Mullings Bradnock, CAE at The Bank of New York Mellon Corp. in New York. “Balancing the activities required to be an assurance function while being a trusted adviser is walking a fine line.”

She says auditors need to show they are team

STRATEGIC THINKING

A horizontal graphic element consisting of a yellow circle on the left, a white circle in the middle containing the text 'STRATEGIC THINKING', and another yellow circle on the right. The circles are partially overlapping and have a white border. The background of the entire page is a teal-tinted photograph of a group of business professionals in a meeting room, sitting around a large conference table with laptops and documents.

A MATTER OF TRUST

players, while retaining their independence. That can involve saying no to myriad stakeholder requests while demonstrating that the function is focused on areas critical to the business strategy.

Having the right team is crucial. “To be a trusted adviser, an internal audit function must have the right complement of talent to address the full spectrum of complex risks within an organization,” she says. That means all auditors on the team need to be conversant with the business, as well as the emerging risks associated with the products and services. “Having the right talent is necessary to deliver on client expectations,” she says. “The full complement

can embrace a wider range of services. That can be hard to achieve, too, but training can help them think differently. Finally, he says, consider moving people out of internal audit who find it too difficult to make the change to a consulting role. One option would be to move them—along with some of the compliance and regulatory work—into the second line of defense, allowing internal audit to focus more in an advisory capacity, he says. “Determining who can make the change, and dealing with those who won’t be able to, can make a difference in successfully creating an audit group that becomes known as a trusted adviser.”

“Auditors are there to make organizations better—it is a key part of the way they can add value.”

— PHILIP RATCLIFFE

A UNIQUE POSITION

Philip Ratcliffe, former president of the Chartered Institute of Internal Auditors and now a consultant who has sat on the audit board of the Biotechnology and Biological Sciences Research Council, sees the role of trusted adviser as providing insights to the board that largely fall outside the normal recommendations that come out of the audit program. That

of individuals with business acumen, industry knowledge, analytical thinking, and strong communication skills are necessary to achieve trusted adviser status.”

Salamasick says those starting out on the route to creating a team capable of providing trusted adviser levels of service are likely to face some stiff challenges. First, he says, try to leverage the technology in the organization so data can be centralized more easily and made more readily available to the audit team. That can take time and money. Second, train the existing team to understand that audit is not just about compliance and assurance, but it

can involve sitting down with the audit committee chair or chief executive and discussing the possible options. “The auditor has to be free to say when something has not worked and to suggest alternative ideas,” he says. “It’s up to management to evaluate that advice and to decide whether to accept it and act on it.”

Auditors may worry that their suggestions don’t work, but Ratcliffe says that may depend on the way management implements their ideas, or some other unforeseen reason. “Auditors are there to make organizations better—it is a key part of the way they can add value,” he says. “Not

INDEPENDENCE



ATTENTION TO DETAIL



VISIT OUR MOBILE APP + InternalAuditor.org to watch a panel discussion on how internal auditors can be viewed as trusted advisers.

commenting when they see a better way to do something could show a certain lack of moral courage.”

Having worked both as a CAE and a nonexecutive director, Ratcliffe says internal audit occupies a unique position within organizations. Because auditors understand the business, know the key people within the organization, and have a firm grasp of where the pressure points are, they are closer in their understanding of how it works than even the CEO. Because the CEO is likely to be more involved with strategic decision-making, that leaves internal audit with an opportunity to give an impartial view to the board on sensitive issues.

“I’m not sure enough internal auditors understand they are in this unique position,” he says. But to take advantage of it, they need to make sure the advice they give is based on facts and arrived at independently. That means undertaking their own risk identification and prioritization exercises and developing views on the culture, morals, and effectiveness of different people in the business.

Ratcliffe stresses that “trusted adviser” implies an informal dimension to the internal audit role that is not covered by the usual range of audit activity. It can, he says, require a lot of tact. If management is incapable of taking remedial action to put controls in place, for example, it may not be something to include in the audit report, but it shouldn’t be ignored.

Trusted advisers need tact, then diplomacy and political awareness, so they understand how people are likely to react when advice is given. Communication skills are key, but so is what Ratcliffe calls communication awareness. That means knowing not just how to say things clearly

and effectively, but to whom you say it and when. He also warns that auditors who do have the ear of the CEO potentially face jealousy or resentment from other managers. He advises them to ensure that their advice is objective and based on facts rather than gut feelings, and to be aware that anything that is said by the auditor in confidence is still likely to become known. “Put a real premium on your modesty and self-restraint,” he says.

PERSISTENT EFFORT

Nobody says that trusted adviser is an easy role to play. Nor is it one where the scope and range of activities can be set in

Trusted advisers need tact, then diplomacy and political awareness, so they understand how people are likely to react when advice is given.

stone. “I spend a lot of time talking with CAEs about these issues,” Kirtley says. “I do think they are fully aligned with my views on how to be a trusted adviser for the audit committee, but it takes diligent attention to detail and constant effort.” And it is a critical one if internal auditors are to be able to provide advice on what keeps their board members awake at night. **ia**

ARTHUR PIPER is a writer who specializes in corporate governance, internal audit, risk management, and technology. He is based in the U.K.



TRUST



See where cyber insights lead

The threat of cyberattacks continues to evolve and intensify. Internal audit can play an integral role in delivering assurance to boards and audit committees on the organization's cyber capabilities. Explore how a cybersecurity assessment framework built on our recommended *Secure. Vigilant. Resilient.*[™] concept can help you address the threats from cyberattacks while delivering value-added insights to your stakeholders.

Read our report on cybersecurity and the role of internal audit.

For more information, contact Sandy Pundmann (spundmann@deloitte.com) or Michael Juergens (michaelj@deloitte.com).

www.deloitte.com/us/CyberIA

See where a new approach to internal audit can take you. See where insights lead.

Deloitte.

Proactive

Fraud Analysis

Integrating advanced forensic data analytics capabilities can help auditors mitigate fraud risks and demonstrate returns.

**Aditya Misra
Vincent Walden**

T

oday's digital world has created new growth opportunities for organizations—but also new fraud risks. Cyber breaches, insider threats, and corruption are among the risks forcing internal auditors to ask new fraud risk questions and seek appropriate technologies to address them. For internal audit departments, forensic data analytics can be a powerful tool for preventing, detecting, and investigating fraud, corruption, and other noncompliant behavior in their organizations.

Investments in such tools are paying off. According to the Association of Certified Fraud Examiners' 2014 Report to the Nations on Occupational Fraud and Abuse, organizations that have proactive data analytics in place have a 60 percent lower median loss because of fraud—roughly US\$100,000 lower per incident—than organizations that do not use such technology. Further, use of proactive data analytics cuts the

median duration of fraud in half, from 24 months to 12 months.

Integrating more mature forensic data analytics capabilities into an organization's audit and compliance monitoring program can improve risk assessment, detect potential misconduct earlier, and enhance audit planning or investigative field work. Moreover, forensic data analytics is a key component of effective fraud risk management as described in The Committee of Sponsoring Organizations of the Treadway Commission's most recent Fraud Risk Management Guide, issued in 2016 — particularly around the areas of fraud risk assessment, prevention, and detection.

A BIG DATA APPROACH TO FRAUD

Fraud prevention and detection is an ideal big data-related organizational initiative. With the growing speed at which they generate data, specifically around the financial reporting and sales activity

When deciding which tests to evaluate, and the corresponding data that will need to be mapped, internal auditors should consider:

What business processes pose a high fraud risk? High-risk business processes include the sales (order-to-cash) cycle and payment (procure-to-pay) cycle, as well as payroll, accounting reserves, travel and entertainment, and inventory processes.

What high-risk accounts within the business process could identify unusual account pairings, such as debit to depreciation and an offsetting credit to a payable, or accounts with vague or open-ended “catch all” descriptions such as a “miscellaneous,” “administrate,” or blank account names?

Who recorded or authorized the transaction? Posting analysis or approver reports could help detect unauthorized postings or inappropriate segregation of duties by looking at the number of payments by name, minimum or maximum accounts, sum totals, or statistical outliers.

When did transactions take place? Analyzing transaction activities over time could identify spikes or dips in activity such as before and after period ends or weekend, holiday, or off-hours activities.

Where do internal auditors see geographic risks, based on previous events, the economic climate, cyberthreats, recent growth, or perceived corruption? Further segmentation can be broken down by business units within the regions and by the accounting systems on which the data resides.

SUCCESS FACTORS

The benefits of implementing a forensic data analytics program must be weighed against challenges such as

Ask the right risk or control-related questions to ensure the analytics will produce meaningful output.

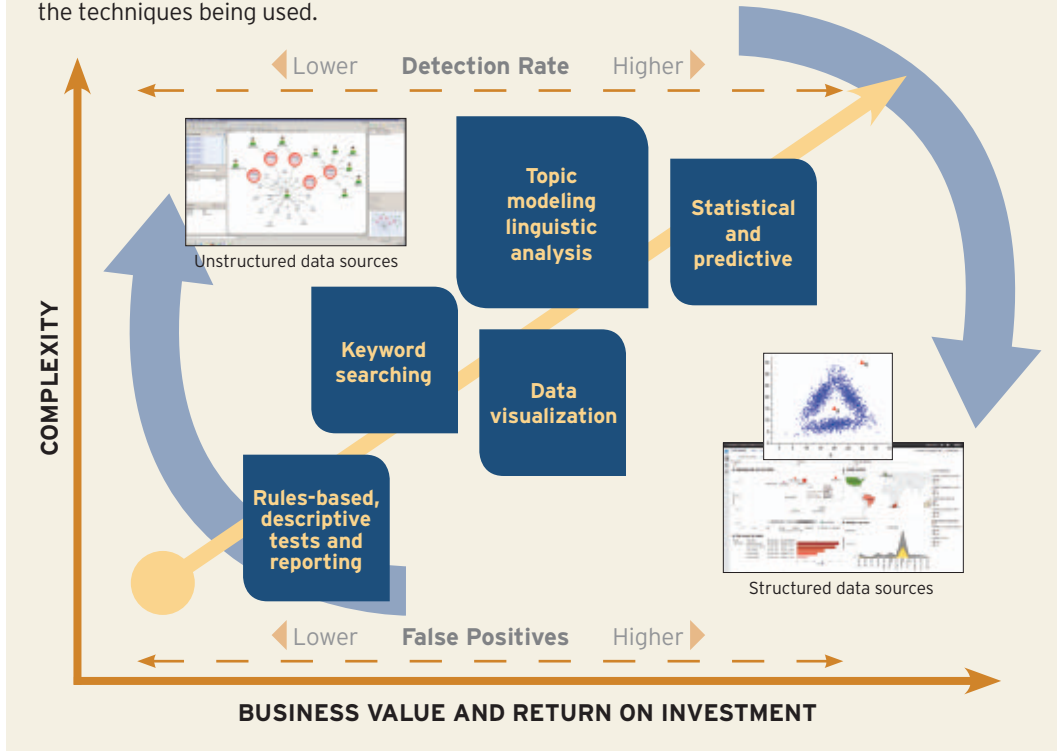
process, organizations — particularly the internal audit function — need ways to prioritize risks and better synthesize information using big data technologies, enhanced visualizations, and statistical approaches to supplement traditional rules-based tests performed in spreadsheet or database applications.

Before jumping into any specific technology or advanced analytics technique, it is crucial to first ask the right risk or control-related questions to ensure the analytics will produce meaningful output for the business objective or risk being addressed.

Three out of five organizations plan to increase their forensic data analytics spending over the next two years, according to EY's 2016 Global Forensic Data Analytics Survey.

FORENSIC DATA ANALYTICS MATURITY MODEL

The model depicted below suggests that as multiple analytics techniques are incorporated, the fraud detection rate increases and the false positive rate decreases, thus improving return on the audit investment. The model also highlights the importance of considering both structured and unstructured data sources as indicated by the blue arrows, regardless of the techniques being used.



obtaining the right tools or professional expertise, combining data (both internal and external) across multiple systems, and the overall quality of the analytics output. To mitigate these challenges and build a successful program, internal auditors should consider five success factors:

Focus on the Low-hanging Fruit

The priority of the initial project matters. Because the first project often is used as a pilot for success, it is important that the project addresses meaningful business or audit risks that are tangible and visible to the business. Further, this initial project should be reasonably attainable, with minimal

capital investment and actionable results. It is best to select a first project that has big demand, has data that resides in easily accessible sources, with a compelling, measurable return on investment. Areas such as insider threat, anti-fraud, anti-corruption, or third-party relationships make for good initial projects.

Go Beyond the Descriptive Analytics

One of the key goals of forensic data analytics is to increase the detection rate of noncompliance, while reducing the risk of false positives. From a capabilities perspective, organizations need to embrace both structured and unstructured data

sources that consider the use of data visualization, text mining, and statistical analysis tools, as shown in the maturity model.

Communication Is Key Internal audit should demonstrate the first success story, then leverage and communicate that success model widely throughout the organization. Results should be validated before successes are communicated to the broader organization. For best results and sustainability of the program, auditors should involve a multidisciplinary team that includes IT, business users, and functional specialists—such as data scientists—who are involved in



We Are Proud to Be Internal Auditors!

As internal auditors, we're proud of our profession. So why not celebrate and help the world understand what internal auditing is all about? It's not about accolades. It's about awareness.

May is International Internal Audit Awareness Month, and The IIA is encouraging members, chapters, and institutes around the globe to spread the message of the value internal auditing brings to an organization and the business community.

Download The IIA's updated Building Awareness Toolkit, featuring creative ideas, tips, tools, and templates for promoting the profession in May and throughout the year.

Mark your calendars for International Internal Audit Awareness Month: **May 2016!**



Show the world you're proud to be an internal auditor with the 2016 International Internal Audit Awareness Month celebration icon!

www.theiia.org/goto/awareness



63% of respondent organizations are investing **at least half** of their forensic data analytics spending on proactive monitoring activities, according to EY's 2016 Global Forensic Data Analytics Survey.

the design of the analytics and day-to-day operations of the forensic data analytics program. It helps to communicate across multiple departments to update key stakeholders on the program's progress under a defined governance regime. Auditors shouldn't just report noncompliance; they should seek to improve the business by providing actionable results.

Involve End-users Leadership support can get forensic data analytics programs funded and set the tone, but the business users—particularly those doing internal audit field work or who are on the front lines of the business—need to adopt it in their daily operations to make the program successful and sustainable. The forensic data analytics functional specialists should not operate in a vacuum; every project needs one or more business champions who coordinate with IT and the business users. Keep the analytics simple and intuitive—don't include too much information in one report so that it isn't easy to understand. Finally, invest time in automation, not manual refreshes, to make the analytics process sustainable and repeatable. The best trends, patterns, or anomalies often come when multiple months of vendor, customer, or employee data are analyzed over time, not just in the aggregate.

Set a Realistic Timetable Enterprise-wide deployment takes time. While quick-hit projects may take four to six weeks, integrating the program can take more than one or two years. Programs need to be refreshed as new risks and business activities change, and people need updates to training, collaboration, and new technologies.


AN OPPORTUNITY FOR INTERNAL AUDIT

As a framework for evaluating the maturity of an organization's use of

forensic data analytics, the "Forensic Data Analytics Maturity Model" on page 35 demonstrates the progression of an organization's maturity journey, starting from rules-based, descriptive tests and reports, to statistical and predictive techniques. Organizations that have implemented forensic data analytics are making strides along the maturity path, according to EY's 2016 Global Forensic Data Analytics Survey of 665 internal audit, legal/compliance, and financial professionals in 17 countries. Respondent

Keep analytics simple and intuitive—don't include too much information in one report so it isn't easy to understand.

organizations conducting forensic data analytics completely in-house increased from 45 percent in 2014 to 67 percent today. Moreover, many of these organizations are expanding their advanced capabilities, such as doubling their use of data visualization tools and incorporating social media and statistical analysis.

Such findings provide evidence of the benefits of integrating advanced forensic data analytics techniques into internal audits. By helping increase their organization's maturity in this area, internal audit has the opportunity to deliver an audit program that is highly focused on preventing and detecting fraud risks. 

ADITYA MISRA, CFE, CPA, is senior manager of corporate audit with Johnson & Johnson in New Brunswick, N.J.

VINCENT WALDEN, CFE, CPA, CITP, is a partner in Ernst & Young LLP's Fraud Investigation and Dispute Services group in Atlanta.



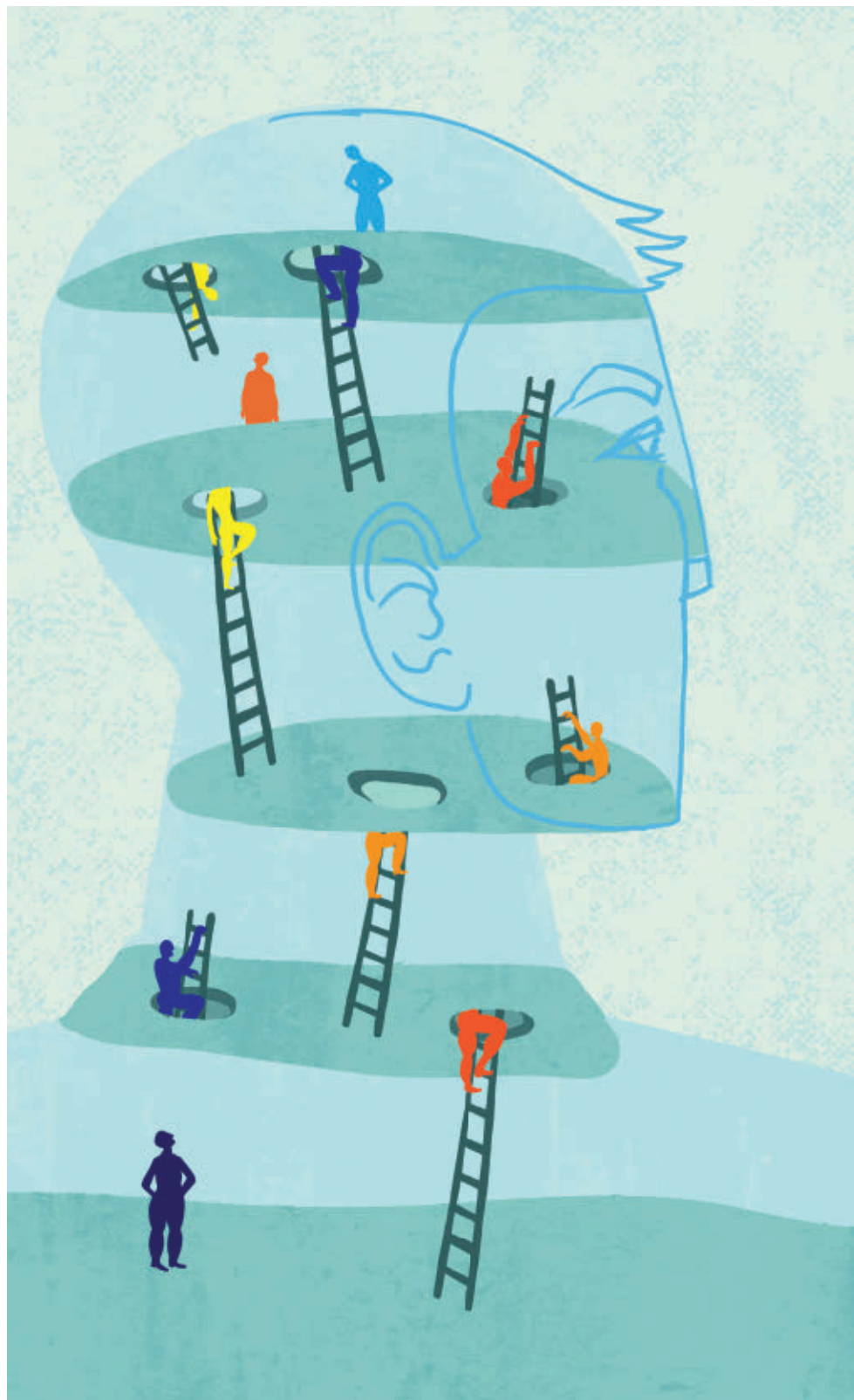
TO COMMENT on this article, EMAIL the authors at aditya.misra@theiia.org

E

xecutives across industries identify communication as one of the most sought after soft skills for their employees. For internal

auditors, one of the key communication skills is interviewing. Successful practitioners can do far more with interviews than just gather information—they leverage the opportunity to gain insight into the way operations work; identify potential successes and failures within those systems; and gauge attitudes about the organization, the process, and internal control environments.

Most auditors are aware of interviewing basics: reviewing documentation before the interview to better understand the area to be discussed, preparing questions in advance, using open-ended questions to elicit more information, using the closing of the interview to verify information gathered, and following up with the



GETTING MORE from interviews

J. Michael Jacka

interviewee on points not covered during the interview. But the most valuable interviews—the ones that allow the auditor to learn more than just the facts—are those that do not feel like interviews. Rather, they become conversations between the auditor and the client. Pioneering talk show host Jack Paar once advised his protégé Dick Cavett, “Don’t do interviews ... interviews are boring. Make it a conversation.” The internal auditor who turns an interview into a conversation will elicit information that can make even the most mundane interview a valuable resource.

KNOWING THE INTERVIEWEE

While obtaining audit-related facts is key to the interview process, knowing about the person being interviewed is equally important. Learning something about the interviewee’s personal life and interests before the interview can

help build a rapport. Familiarity with the individual’s personality, as well as his or her perceptions of internal audit, can also help the auditor develop an effective approach to the interview and prepare for potential challenges.

To learn more about the interviewee, the auditor should talk to others within the audit department. Is he or she forthcoming with information? Does it take time for the interviewee to warm to the interview process? Does he or she dislike small talk and prefer to get to the substance of a discussion as quickly as possible? Anyone in the audit department who has previously worked with the interviewee should be able to provide such insights. Contacts outside the audit department can help supply this information as well.

PURPOSE

Many auditors fall into the trap of interviewing without first identifying

Instead of emphasizing formalities, internal auditors should approach each interview like a conversation.

a key point—the interview’s purpose. Even if the purpose is as simple as “gather information about the process” or “determine the reason controls have been ineffective,” articulating it will aid interview preparation and execution. The purpose should be explained before the meeting, enabling interviewees to prepare adequately, understand their role in the process, and recognize the value of their requested contribution.

Each interview’s purpose should be specific, attainable, and outcome-oriented. To state the purpose as “to understand how the accounts payable supervisor controls operations” is

Letting the interviewee know what to expect can go a long way toward reducing his or her stress.

fine, though a better purpose statement would be “to understand the accounts payable supervisor’s role in ensuring the timely and accurate payment of expenses and to determine operating efficiencies, issues, and potential improvements.” The latter positions both the auditor and the interviewee to better focus on what will be achieved.

THE COMFORT ZONE

Good interviews are more likely to occur when the interviewee feels at ease. A nervous or tense interviewee usually gives terse, incomplete answers. Auditors can address uneasy feelings by helping interviewees prepare for the interview, being mindful of the interview location, and choosing an effective way to open the discussion.

Preparation Before the interview, interviewees should be given sufficient

information to understand why the interview is occurring, how their participation will help the audit process, and what information they will need to provide. Details should include who will be in the interview, any documents that might be required, and, as noted earlier, the interview’s purpose. Letting the interviewee know what to expect can go a long way toward reducing his or her stress.

Location To further set the client at ease, most interviews are held in the interviewee’s office or work area. Pulling employees from their normal workspace only reinforces potential fears that the auditors may have ulterior motives. Interviewees are more likely to engage in a fuller, more complete conversation when they are in a familiar setting.

At the same time, interviews should take place in a location where the interviewee can provide open, honest answers. If the discussion might be overheard, the interview should be moved to a more private location that is still familiar to the client—a nearby meeting room, for example. Some auditors sacrifice privacy to ensure interviewees have easy access to any documents the auditor may request. However, privacy is always preferable. Documents can always be obtained later, but the auditor usually has only one chance for a frank and candid conversation.

Opening The opening of the interview sets the tone for the rest of the discussion. Auditors must use what they learn in advance about the interviewee to determine how to start the conversation in a way that will put him or her at ease. If the individual has never been interviewed by internal audit before, extra time should be spent to explain the purpose and expected outcome of the interview. If

95% of respondents from The IIA's 2016 North American Pulse of Internal Audit survey indicate that their audit function is currently either training or recruiting for active listening skills.

QUESTIONS THAT ELICIT INFORMATION

Before the interview, auditors typically prepare sets of questions designed to gather specific information for the audit. Several well-phrased, general questions can help the auditor move the conversation forward, dig deeper into the area under consideration, and help elicit more meaningful responses from the interviewee. Although they should not all be used in every interview, and may need to be used sparingly to avoid focusing on the questions rather than the answers, having these questions available will improve the quality of most interviews.

Insight into the person and the job

- » How long have you worked in this position?
- » How did you learn to complete this process?
- » What is your favorite part of this job?
- » How many other people are in this same role?
- » What is your proudest achievement in this role?
- » Do others in the organization recognize your department's achievements?

Insight into the process

- » What do you do next?
- » Why do you do this?
- » How has the job changed over the last few months?
- » Who are your main customers/vendors?
- » What is the most difficult task you have to perform?
- » Who else should I talk with?

Insight into the controls

- » What is the worst that can happen?
- » How do you/your boss make sure this gets done?
- » How much training is required?
- » How is your/your department's success measured?

Insight into improvements

- » How would you change this?
- » What is going right? What is going wrong?
- » What is the most time-consuming activity?
- » Do you have enough understanding/autonomy/authority to do your job?
- » Do you have the resources you need to do your job?

At the end of the interview, the auditor also needs to ensure interviewees have had the opportunity to share all the information they wanted to share. Powerful final questions include, "Is there anything else you would like to add?" and "Is there anything you wish I had asked?" The first question allows interviewees to reflect on the discussion, and the second allows them to go beyond the parameters of the interview and freely discuss other issues or concerns they may have.

he or she has had a negative experience with internal audit in the past, then the auditor must devote extra effort to show that the experience was an aberration. Most importantly, the auditor should use the opening to establish a connection with the interviewee. Casual conversations seldom begin by asking someone about his or her personal life, and interviews should not begin by asking, "What would you say ... you do here?"

LISTENING

Many auditors forget that, before the profession co-opted the word, an auditor was "a listener." In fact, more than any other factor, effective interviewing hinges on the auditor's ability to listen. Successful interviews are more likely to occur when the auditor spends no more than 30 percent of his or her time talking and the remainder listening to what the interviewee has to say. Author Tom Wolfe said, "The world is full of people with information compulsion who want to tell you ... things that you don't know. They're some of the greatest allies any writer has." Once interviewees feel at ease, they will often provide more information than the practitioner expects. All he or she has to do is listen.

Effective listening occurs when the auditor allows the interviewee to answer questions completely without interruption, does not react judgmentally to the answers, and listens for more than just the words being said. The auditor should focus on the message conveyed by the interviewee. Sometimes that message may have little to do with the questions asked, but it may be more important than the facts the auditor originally sought.

Several factors can inhibit the auditor's ability to "hear" the client's message. These include thinking about the next question to be asked,

reflecting on how the answer impacts previous answers, ensuring the direction of the questioning fits the overall purpose of the interview, wondering if the information being given is factual, focusing on the time remaining for the interview, and even dwelling on mundane issues such as hunger, stress, and personal matters. In fact, similar distractions may be impacting the interviewee's ability to provide information to the internal auditor.

To better focus on what interviewees say, auditors should use active listening techniques (see "Active Listening," this page). These include maintaining appropriate eye contact, using attentive silence, encouraging the interviewee to continue, and summarizing his or her answers. Each of these techniques serves to ensure the auditor understands what the interviewee has said and reassure the interviewee that the information he or she has shared is of value.

QUESTIONS AND FLEXIBILITY

When preparing for the interview, the auditor should determine the general information needed to fulfill the interview's purpose. From this foundation, specific questions can be developed, though the auditor should not rely too heavily on those questions. News person Katie Couric once said, "Nothing is worse for me as a viewer than to watch someone go down a laundry list of questions and not explore something with a little more depth. ... You need to use your questions as sort of a template, but you have to be willing to listen and veer off in a totally different direction." When auditors rely on scripted questions, they limit the exchange of information and are more apt to miss opportunities for the conversation to go in unexpected but valuable directions.

Flexible listening is the art of recognizing when there is value in letting

ACTIVE LISTENING

Active listening involves making a conscious effort to hear not only the words being said, but the complete message being delivered. It is accomplished through the use of techniques that focus the listener on the message and provide interviewees with the comfort that their message is being received. The approach consists of three main components:

Attending

Giving the interviewee undivided attention with limited interruptions.

- » Establish a nondistracting environment.
- » Put aside distracting thoughts.
- » Refrain from preparing mental rebuttals.
- » Be sensitive to the interviewee's style and approach.
- » Adopt an appropriate nonverbal posture for listening.
- » Maintain eye contact.

Following

Using body language, gestures, and phrases to convey attention.

- » Maintain attentive silence.
- » Encourage the interviewee to continue with small verbal comments.
- » Nod occasionally, smile, and use other supporting facial expressions.
- » Observe nonverbal cues and check for incongruities.
- » Ask clarifying questions.
- » Find common ground for discussion.

Reflecting

Ensuring that the message received matches the one delivered.

- » Summarize ("So, what you are saying is ...").
- » Paraphrase ("It sounds like you are saying ...").
- » Link perspectives ("What I am hearing is ...").
- » Reflect feelings ("So, you seem to feel ...").

the interview veer in those directions. It comes from listening to more than just the words and paying attention to the tone, pauses, and nuances of the answer—what is being left unsaid. Based on this information, the auditor knows to either move on to the next subject or dig deeper. Flexible listening helps inform the direction of the interview and discourages reliance on preconceived notions about what the discussion will consist of.

At the interview's conclusion, the auditor can go back to his or her

specific, prewritten questions and ensure all necessary areas have been covered. If something has been missed, the interview should continue, and the auditor should be prepared for the unexpected answer that may lead to more valuable information.

RAPPORT

The key to turning an interview into a conversation is establishing a rapport—in fact, much of the preceding discussion has focused on practices aimed at doing just that. But rapport is



as much about the overall perceptions of the auditor and the audit department as it is about the interview. Everything everyone within the department does helps establish or destroy those perceptions.

It begins with auditors seeing interviews as not just another part of the audit, but as a stepping stone in establishing a rapport with fellow employees. Moreover, practitioners must recognize that the interview is really about the people involved, not just the information needed. Auditors who explain to an interviewee that the interview must be done to complete the audit reveal an inappropriate focus and provide no value proposition for the interviewee.

Interviews are also more effective when the auditor demonstrates a curiosity for learning. Author Courtney Seiter notes, “A true passion for learning about those around you goes further than any trick or even the most polished communication skills.” Auditors should be curious about the way processes work, the way the organization works, and perhaps most importantly, the people who make it work. Curiosity will lead to a better understanding of the organization, better ideas for improving the organization, and a better rapport with the individuals within the organization.

Finally, auditors should take every opportunity to get to know potential interviewees outside of the audit experience. As Tom Peters says, “‘Do lunch’ with people in other functions! Frequently!” The more people connect with internal auditors as fellow employees, the more likely they are to provide genuinely valuable information during an interview.

PRACTICE, PRACTICE, PRACTICE

Becoming a better interviewer starts with understanding the basics and continues with grasping the nuances

that make interviews a real conversation. One way to learn is by watching others. Director Quentin Tarantino says, “When people ask me if I went to film school I tell them, ‘No, I went to films.’” Similarly, auditors can watch interviews—those conducted by other auditors and those conducted by professional interviewers—to learn what works in practice and what doesn’t.

Interviews are more effective when the internal auditor demonstrates a curiosity for learning.

Next, internal auditors should practice what they’ve learned, though not necessarily as part of an audit. To build rapport, auditors can just talk to people in the organization informally. They can explain that the discussion has nothing to do with audit; the purpose is to learn about the organization and the people who work there. As noted previously, people love to talk about themselves—with no more agenda than being curious about the work and the people who do that work, auditors can practice becoming a better interviewer.

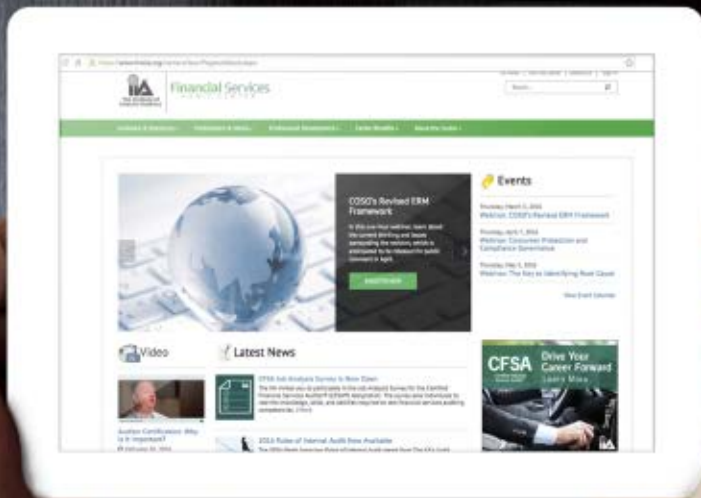
Ultimately, the auditor who approaches an interview with the idea of establishing a better rapport, using active listening skills, and just letting the interviewee talk will see the discussion turn from an interview to a conversation. And in the process, the auditor will gain more information than a formal, pre-scripted interview could ever yield. [ia](#)



TO COMMENT
on this article,
EMAIL the
author at michael.jacka@theiia.org

J. MICHAEL JACKA, CIA, CPCU, CFE, CPA, is cofounder and chief creative pilot for *Flying Pig Audit, Consulting, and Training Services* in Phoenix.

You Face Unique Challenges in Financial Services



Here Are the Tools and Resources to Tackle Tomorrow's Demands.

As the demand for top talent and acumen in the financial services industry rises, how do you differentiate yourself from your peers?

Stand Out With Your CFSA Apply in April and Save Up to US\$200!*

There is no better way to establish your credibility than with the Certified Financial Services Auditor® (CFSA®) designation. Earning the CFSA demonstrates your commitment and quickly communicates your breadth of knowledge to tackle unique challenges. Submit your application by April 30 and we will waive the fee, saving you up to US\$200 at www.theiia.org/goto/CFSA.

Influential. Impactful. Indispensable. The Financial Services Audit Center

The needs of financial services auditors have grown in complexity due to increased pressures from regulators. If your audit team not only answers to your board and management, but also to the Federal Reserve, OCC, CFPB, SEC, FINRA, or state banking or insurance regulators, then the Center is designed for you. Add the Center to your IIA membership today at www.theiia.org/FSAC.

*This offer applies only to the CFSA application fee. This offer may not apply in countries where exams are administered through institutes with certain agreements. Please contact your local institute to verify if the offer is valid in your country. Excludes exam registrations.

Taking a close look at payroll risks can enable internal auditors to help their organizations save money and identify wrongdoing.

**Christopher Kelly
Frans Deklepper**

Payroll can amount to 40 percent or more of an organization's total annual expenditures. Payroll taxes, Social Security, Medicare, pensions, and health insurance can add several percentage points in variable costs on top of wages. So for every payroll dollar saved through audit identification, bonus savings arise automatically from the on-top costs calculated on base wages.

Different industries will exhibit different payroll risk profiles. For example, firms whose culture involves salaried employees who work longer hours may have a lower risk of payroll fraud and may not warrant a full forensic approach. Organizations may present greater opportunity for payroll fraud if their workforce patterns entail night shift work, variable shifts or hours, 24/7 on-call coverage, and employees who are mobile, unsupervised, or work across multiple locations. Payroll-related risks include over-claimed allowances, overused extra pay for weekend or public holiday work, fictitious overtime, vacation and sick leave taken but not deducted from leave balances, continued payment of employees who have left the organization, ghost employees arising from poor segregation of duties, the vulnerability of data outputted to the bank for electronic payment, and roster dysfunction.

Yet the personnel assigned to administer the complexities of payroll are often qualified by experience more so than by formal finance, legal, or systems training,

On the Hunt for **Payroll Fraud**

thereby creating a competency bias over how payroll is managed. On top of that, payroll is normally shrouded in secrecy because of the inherently private nature of employee and executive pay. Underpayment errors are less probable than overpayment errors because they are more likely to be corrected when the affected employees complain; they are less likely to be discovered when employees are overpaid. These systemic biases further increase the risk of unnoticed payroll error and fraud.

All these factors make assuring payroll controls entail a great deal of

One way to analyze payroll cost is through a distribution analysis of aggregate salary data. This can be obtained by stratifying 12 months of earnings by individual employees in a distribution chart, to show the composition of salaries across the entire workforce, from the small number of highly paid executives to lower-paid, unskilled labor (see “Distribution of Total Payroll Costs” on page 47). Typically the distribution will skew to the left because not all employees will have worked a full 12 months. Some employees may have joined or departed the organization during the year, and not all employees will be employed full-time. What this chart shows is how the mean salary level compares to the industry and whether or not the shape of the distribution is what management would expect.

An insightful audit test can be to ask management how it expects salaries to be distributed above and below the average. For instance, the two peaks shown in the chart reveal that many employees were paid close to the average (the left peak), while a significant number were paid well above average (the right peak). Further analysis will reveal how this is attributed to additional earnings such as overtime, late night or weekend pay, and allowances.

Using the same source, departmental data concentrations can be graphed in a bubble chart where each bubble represents a department or cost center (see “Average Total Payroll Cost by Department” on page 48). These charts highlight areas for audit questioning, such as where weaknesses in internal control may have permitted some employees to be overpaid.

Remuneration Payroll data analysis can reveal individuals or entire teams who are unusually well-remunerated because team supervisors turn a blind eye to payroll malpractice, as well as

Internal auditors may add greater value by launching the audit with a top-down analysis of total payroll cost.

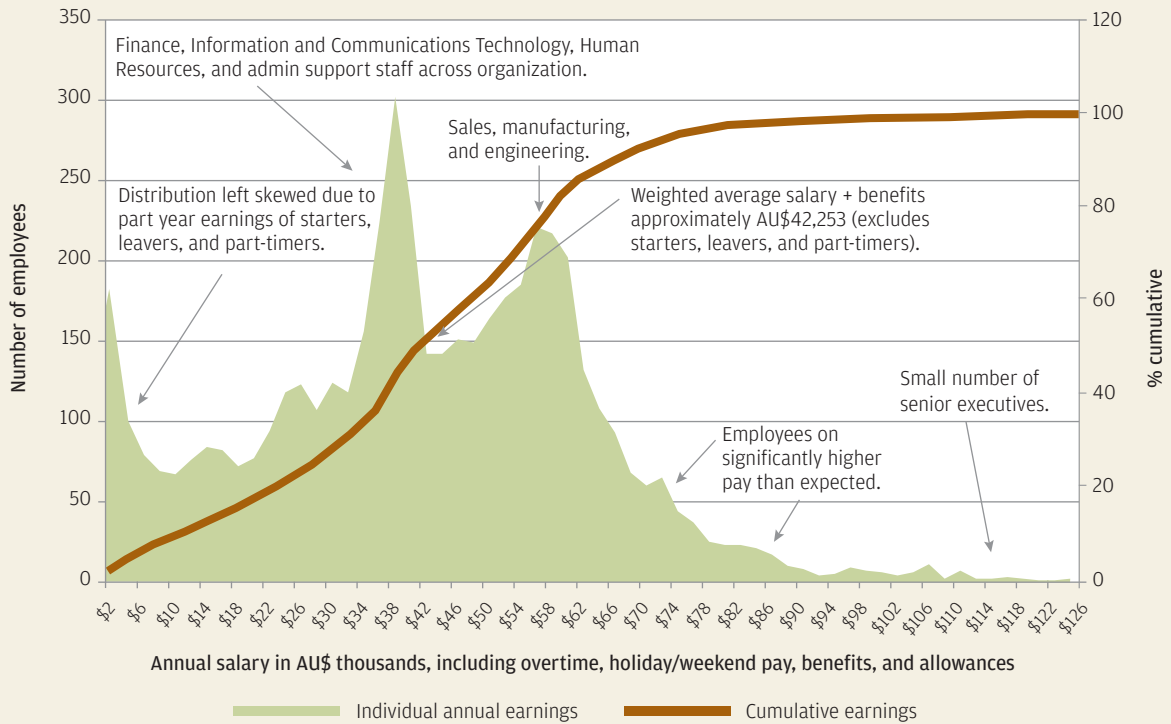
audit work that can easily leave auditors disoriented in details. Payroll risk’s silver lining is that it can provide opportunities for auditors to uncover actual cost savings and labor productivity gains.

HELICOPTER ANALYSIS

It is tempting to start a payroll review by auditing payroll compliance, such as checking that salary rates are in accordance with appropriately authorized contracts or checking that time sheets agree with clock in/out times. However, internal auditors may add greater value by launching the audit with a top-down analysis of total payroll cost and using that perspective to inform the detailed tests needed to provide assurance about the effectiveness of controls around the most crucial risks. If auditors omit a helicopter overview of payroll data and the payroll process, they risk performing detailed work where it is less needed while missing out on significant discoveries.

The average payroll fraud incident lasts **24 months** and costs **US\$50,000**, notes the Association of Certified Fraud Examiners' 2014 Report to the Nations on Occupational Fraud and Abuse.

DISTRIBUTION OF TOTAL PAYROLL COSTS



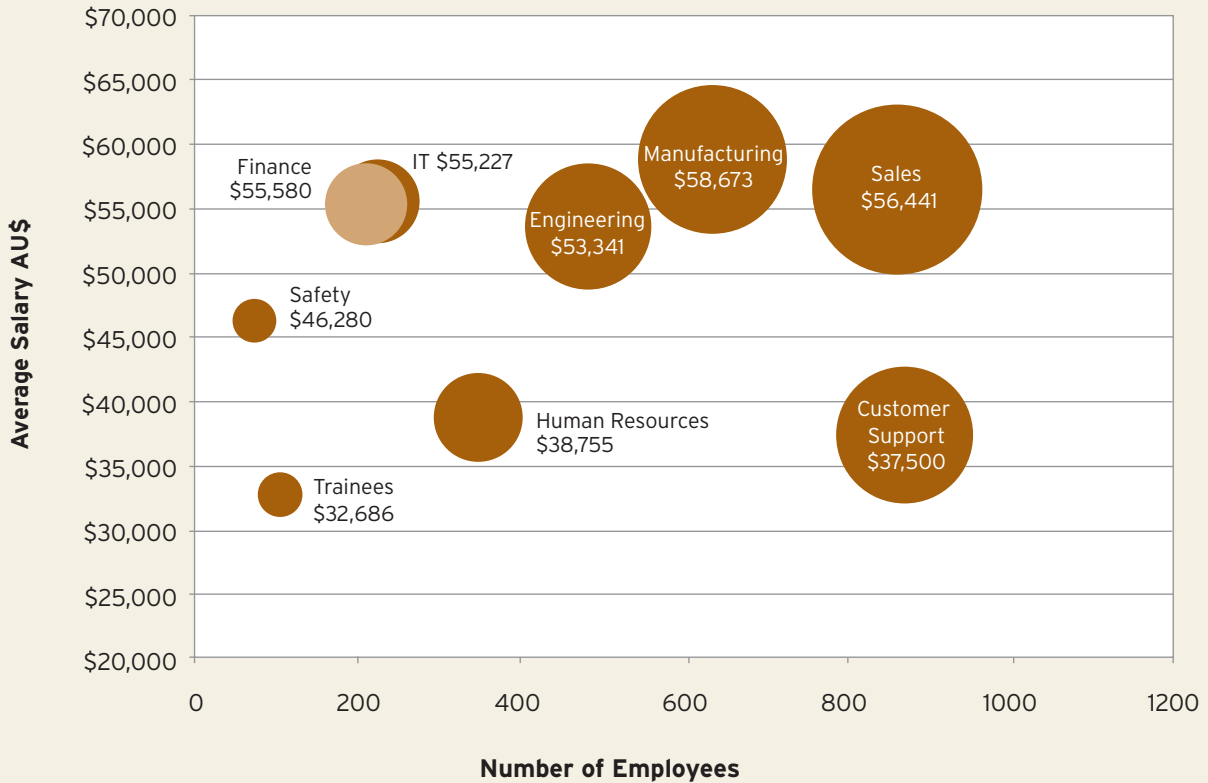
low-remunerated personnel who represent excellent value to the organization. For example, it can identify the night shift worker who is paid extra for weekend or holiday work plus overtime while actually working only half the contracted hours, or workers who claim higher duty or tool allowances to which they are not entitled. In addition to providing management with new insights into payroll behaviors, which may in turn become part of ongoing management reporting, the total payroll cost distribution analysis can point auditors toward urgent payroll control improvements.

Rosters Process analysis also can help steer the detailed audit test program. A payroll process overview can encompass how staff duty rosters, or schedules,

are kept updated with operational needs, daily time and attendance controls, overtime approval, time sheet data entry, employee sick leave, leave approval, and how internal controls can potentially be overridden. The data on which pay is calculated originates in these often manual subprocesses, which are reliant on employee honesty and are vulnerable to error and fraud, translating into real payroll dollars.

Rosters should be designed to optimize the allocation of employees to operational needs. If done well, rosters should eliminate, or at least minimize, the need for overtime and weekend work. Therefore, if the analysis of earnings across the workforce shows departments where overtime, holiday, or weekend bonus pay is higher than expected, this might

AVERAGE TOTAL PAYROLL COST BY DEPARTMENT



indicate roster dysfunction, neglect of internal controls, or under-staffing. The helicopter overview may identify business units that require special audit examination.

Process Efficiency Similarly, the efficiency of the payroll process can be considered. Organizations sometimes run multiple payroll processes across different sites such as between white-collar and blue-collar workforces or arising from historic business mergers. Efficiency savings may be achievable through collapsing multiple payrolls into a single cycle. At one organization, auditors found that the monthly executive mid-month payroll cycle was easily collapsed into the biweekly

cycle, which canceled 12 pay cycles per annum and eliminated risks around paying executive employees half a month's wages in advance. The changeover also increased the accuracy of the attendance and leave recording, because all employees went onto the same fortnightly pay cycle. Permanent efficiency savings like this are a tangible way for internal audit to add value.

DISCOVERING DIAMONDS IN THE DETAIL

Using the helicopter overview to generate insights into the payroll subprocesses most vulnerable to fraud and error can position internal audit to mine the rich payroll data to either assure the board that all is well or



TO COMMENT on this article, EMAIL the author at christopher.kelly@theiia.org

Payroll fraud comprises **16%** of fraud in small businesses and **8%** in other companies. It's most common in religious, charitable, and social service organizations, the 2014 Report to the Nations notes.

DATA MINING TIPS

Downloading and analyzing data across multiple sources is not easy, but doing so can be a worthwhile investment in enhancing audit effectiveness. Depending on internal audit's organizational status, access to data may need to be negotiated with the relevant custodians, subject to local privacy restrictions and audit right of access.

Once obtained, downloaded data usually arrives in disparate formats, most commonly text (TXT, RTF) or comma-separated values (CSV), which in turn may be variously imported into Microsoft Excel or other spreadsheet software in ways that impede audit analysis. For example, data containing numbers with slashes or hyphens may be converted into dates, and numbers and colons may be converted into time values.

Data containing characters deemed as wildcards by Excel, such as "*" and "?" may need to be replaced (using "~") to ensure Excel does not treat the character as a wildcard. Numbers with leading zeros such as telephone numbers may be imported as integers with the leading zeros truncated, making them difficult to cross-match with a telephone directory.

Time Data mining envisaged here often involves the analysis of time, which can be complicated in Excel. For analyzing time sheets and clock in/out data, Excel's DATEVALUE() and TIMEVALUE() functions can assist with converting cells containing a mix of date and time into date-only or time-only values either in AM/PM or 24-hour clock format, which can then be sorted and analyzed. Excel does this by dividing each second into one 86,400th of a day—that is 60 seconds x 60 minutes x 24 hours. So 1/86,400 is one second after midnight, 86,399/86,400 is one second before midnight, and 0.5 is midday. Complementary to that, dates in Excel are numbered in positive integer sequence from 1 (Jan. 1, 1900). So logically, the date value is the positive integer and the time value is the decimal component. Both dates and times can then be sorted and used in calculations and pattern-seeking, which can then be presented back to management as a candlestick chart showing actual hours worked compared to the day-by-day rostered shift over a period of several weeks or months.

Telephone numbers Telephone numbers can present another challenge because Excel automatically imports

numeric strings as numbers, whereas auditors may prefer to use telephone numbers as text strings for sorting and lookup. When importing, Excel can also misinterpret the international telephone dialing symbol "+" as a mathematical operator. If telephone call logs are being matched against an electronic telephone directory, the auditor may need to convert all telephone log data into text format to preserve leading zeros; otherwise they will be truncated and mismatched if the imported telephone data is converted to numeric format. To avoid Excel stripping the leading zeros, telephone numbers can be preceded by an apostrophe ('), using the CONCATENATE() formula, or by using Excel's TEXT(cell_ref, "#") formula where "#" can be substituted with a variety of syntaxes. Parsing is another technique if data fields contain consistent patterns of numeric and alphabetic data. If all else fails, it may be easier to trim all leading zeros in both the telephone log data and the lookup table by treating both as numeric fields rather than text. Once telephone call data is obtained, it can be traced to available phone number lists. Even Google yields a surprising amount of information if auditors type in a telephone number.

Email Data associated with email can provide both date and time of day transactional information as well as the content of the written messages, themselves. Email software such as Microsoft Outlook often enable users to export entire mailboxes as plain text, comma-separated files, Excel-readable files, and other formats for advanced searching.

The above are just some of the ways to scrub data before audit analysis. In the event the data needs to be recreated at a later date—for example, if a legal situation arises—it is helpful to ensure the data-scrubbing methodology is documented in the internal audit workpapers. Over time, this array of cleansed data can become a valuable research lab kept up to date to support future audits.

Compiling and analyzing data is worth the effort. Findings informed by the organization's own data become harder to refute. Sometimes findings can be sufficiently startling that management will implement audit's recommendations quickly and decisively to show they have corrected the problems.

otherwise expose potential wrongdoing. Available data likely includes each employee's start time, finish time, hours worked, location worked, vacation dates, sick time, standard pay rates, night-shift pay rates, overtime pay rates, and allowances. To accommodate the volume of data, payroll systems typically contain a job position master file, employee master file, and time sheet transaction history holding all hours worked as well as leave, which in turn update balances across all leave types. Additionally, the organization's human resource systems may hold data on performance appraisals, competencies, and disciplinary history that frequently is

disciplinary records. Or, auditors could invert those factors to find the unrecognized exemplary performers.

Where audit findings suggest fraud concerns about identified employees, internal audit can add value by triangulating time sheet claims against external data sources such as site access biometric data, company cell phone logs, phone number caller identification, GPS data, company email, Internet usage, company motor fleet vehicle tolls, and vehicle refueling data—most of which contain useful date and time-of-day parameters (see "Data Mining Tips" on page 49). Before taking this approach, CAEs should consider the audit committee's risk appetite, internal

deducting leave taken and overstating leave balances.

- » Employees who moonlight in businesses on the side during normal working hours, sometimes using the organization's equipment to do so.

The problems are magnified where supervisors collude with their employees by approving exaggerated time sheets and perpetuate the culture by inducing others to engage in what auditors may see referred to as "custom and practice." When analyzed systematically and corroborated with other intelligence such as whistleblower information, these disparate data sources can reveal systemic fraud.

Management welcomes findings that reveal specific wrongdoing because they provide hard-to-dispute evidence.

linked to the employee number used for payroll purposes.

The detail inside these databases can reveal hidden information. Who are the highest earners of overtime pay and why? Which employees gained the most from weekend and public holiday pay? Who consistently starts late? Finishes early? Who has the most sick leave? Although most employees may perform a fair day's work, the audit analysis may point to those who work less—sometimes considerably less—than the time for which they are paid.

Joined-up query combinations to search payroll and human resources data can generate powerful insights into the organization's worst and best outliers, which may be overlooked by the data custodians. An example of a query combination would be: employees with high sick leave + high overtime + low performance appraisal scores + negative


audit's data access rights, and local privacy laws.

The data buried within these databases can reveal employee behavior, including what they were doing, where they were, and who they were interacting with throughout the work day. Common findings include:

- » Employees who leave work wrongfully during their shift.
- » Employees who work fewer hours and take sick time during the week to shift the workload to weekends and public holidays to maximize pay.
- » Employees who use company property excessively for personal purposes during working hours.
- » Employees who visit vacation destinations while on sick leave.
- » Employees who take leave but whose managers do not log the paperwork, thereby not

MAKING A DIFFERENCE

Often management welcomes audit findings that reveal specific wrongdoing because they provide hard-to-dispute evidence with which to remedy low-performing teams, discipline or terminate unproductive personnel, and sharpen finance and management focus on cost control. These are audits that make an impact.

Well-researched and documented audit fieldwork can support management action against those who may have defrauded the organization or work teams that may be taking inappropriate advantage of the payroll system. Simultaneously, internal auditors can partner with management to recover historic costs, quantify future savings, reduce reputational and political risk, improve the organization's policies, and boost the productivity and morale of employees who knew of the wrongdoing but felt powerless to stop it. 

CHRISTOPHER KELLY, DPROF, FCA, is partner with Kelly & Yang based in Melbourne, Australia.

FRANS DEKLEPPER, is senior software engineer at Callista Software Services in Melbourne.

UNDERSTAND RISK

Identification

Quantification

Decision Making

Messaging



ENTERPRISE RISK MANAGEMENT

Master of Science | Certificate | Courses

Columbia University has developed a portfolio of offerings in Enterprise Risk Management (ERM) that will prepare risk professionals in public and private organizations with knowledge of ERM practices, tools, and techniques, and an ability to adapt the appropriate ERM framework to integrate properly with existing risk infrastructure.

MAY
15

MS Fall 2016 Application Deadline

Learn more SPS.COLUMBIA.EDU/ERM316

GUARDIANS OF INTEGRITY

Michael Brozzetti

Internal audit can provide insight into corporate integrity and people-related risks.

Integrity is defined as the firm adherence to moral and ethical principles. Ethics and morals establish criteria to evaluate right and wrong behavior; however, they differ in that morals reflect an individual's values, and ethics reflect the broader value system established by a society, institution, or organization.

In an organization, ethics are often codified within a code of ethics or code of conduct and adopted by the governing board and senior management. Organizational integrity will never rise above the integrity of the people who create, administer, and monitor the internal control system. Assessing organizational governance can help provide assurances that internal controls are designed and operating within an environment that promotes the ethics and values of the organization. Though The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) provides guidance on the

internal auditor's role in governance (Standard 2110: Governance), the implementation of the *Standards* must be adapted as technologies evolve and societies change.

INTERNAL AUDIT AS CORPORATE CONSCIENCE

The internal auditor is wise to consider the organization's mission and values when discerning the decisions and actions made by those entrusted to govern and manage the organization. Standard 2110 states, "The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.



- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.”

In the area of ethics, the internal audit department may perform the role of corporate conscience and must be in a position to influence the corporate “brain,” which includes the board and management. Just as a conscience guides an individual’s actions, internal audit guides the actions of a corporation by providing insight and advice to the board and management, who are the keepers of the organizational body and the

ethics are incident reporting and resolution and cultural risk intelligence.

Incident Reporting and Resolution

When evaluating the incident reporting and resolution process, internal auditors should have insight into the organization’s expectations. For example, has management designed a process to identify and address all behavior that is inconsistent with the organization’s code of ethics and policies, professional standards, regulations, and laws? Or is the process designed to address only those matters related to financial reporting fraud to comply with the law?

Understanding how the organization defines success is essential because it establishes the criteria used to evaluate alleged acts of wrongdoing within the context of the internal ethics systems, the external legal system, or both. Evaluating alleged acts of wrongdoing against the code of ethics first demonstrates the organization’s commitment to an ethical culture well beyond the minimal standards set forth by laws and regulations. This approach also allows the organization to identify and resolve business issues before they grow into potentially larger and more complex legal issues.

The incident reporting and resolution process often involves multiple stakeholders, including management, human resources, legal, compliance, ethics, and internal audit. When determining whether the parties reviewing incident reports are competent, independent, and free from any potential conflict of interest, the internal auditor may opine upon whether the reports’ design supports due process for the parties involved. In addition, the internal and external informants should be made aware of their duty to provide complete and useful information, the responsibilities of those reviewing the reports, and

The outcome of every incident report reflects directly on how well the process is designed and operating.

trusted guardians of its well-being. As the corporate conscience, internal auditors must be prepared to have open, candid, and constructive dialogue with the board and management, not only to comply with the *Standards*, but also to ensure the organization finds the right balance between financial and ethical performance.

SAFEGUARDING THE ORGANIZATION’S INTEGRITY

Internal auditors often assess the design of ethics-related programs and activities easily. One example is verifying that a code of ethics is documented and approved or that a hotline exists and is available for reporting incidents. However, testing the effectiveness of programs and activities is often more challenging. Two key areas for the evaluation of

53% of CAEs polled in the 2016 North American Pulse of Internal Audit report find it “very” or “extremely” effective to coordinate with other governance functions to address toxic culture.

UPHOLDING THE CODE OF ETHICS

Strong political or cultural pressures that directly conflict with internal auditors’ duty to uphold The IIA’s Code of Ethics and the profession’s principles of integrity, objectivity, confidentiality, and competence may challenge them, making sound discretion and judgment essential.

Integrity Internal auditors’ commitment to integrity establishes the basis for trust and reliance on their judgment. This principle requires auditors to perform tasks honestly, diligently, and responsibly, and, consequently, to contribute to the legitimate and ethical objectives of the organizations they serve. Integrity also requires internal auditors to make appropriate disclosures as required by law and expected by the profession, and to avoid participating in illegal or discreditable acts. As an ultimate safeguard to integrity, internal auditors can save and maintain a personal cash reserve so if they are faced with a situation that could compromise their integrity, they can resign without the fear of financial hardship. Maintaining a personal cash reserve to cover at least six months of living expenses will help an internal auditor maintain sound discretion and judgment when confronted by ethical dilemmas.

Objectivity Internal auditors must exhibit the highest level of professional objectivity when gathering, evaluating, and communicating information about the activities being examined. When forming judgments, practitioners maintain professional objectivity by making a balanced assessment of all relevant circumstances and avoiding the undue influence of the interests of themselves or others. The core of this principle lies in the disclosure of material facts when reporting; managing conflicts of interests, whether they exist in fact or in appearance; and maintaining an unbiased mental attitude while performing audit work. Internal auditors can achieve high levels of professional objectivity when they embrace the principle of integrity and genuinely believe in the scope, nature, and extent of the work they are performing, rather than merely accepting the direction of others without exercising discretion and judgment.

Confidentiality Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so. Core to this principle is the ability to balance strict confidentiality with those circumstances that may call for the disclosure of information outside ordinary communication channels to protect the legitimate and ethical objectives of the organization. Serving an organization as an internal auditor requires loyalty to the organization as a whole, taking into account its many stakeholders. The discretionary authority to determine a professional disclosure obligation will continue to emerge as the profession becomes universally recognized and accepted as serving a public good.

Competence Internal auditors apply the knowledge, skills, and experience needed to perform internal audit services. This principle requires them to provide services only in areas where they have the requisite expertise. This means applying the *Standards* and continually improving their proficiency and the quality of their work through learning and education. In addition to participating in formal learning opportunities, the internal auditor may also recognize the informal chances to learn from daily interactions with peers, colleagues, and constituents throughout all levels of an organization.



TO COMMENT
on this article,
EMAIL the
author at
michael.brozzetti
@theiia.org

the follow-up protocols. For example, informants should be encouraged to identify the related provision of the ethics code, policy, or regulation that they believe is compromised and the evidence to support their report. This detailed information could improve the quality of the incident report and greatly reduce the cycle time for a comprehensive review and resolution.

The outcome of every incident report reflects directly on how well the process is designed and operating. It

group or individual within the organization. Just as internal auditors are considered the eyes and ears of the governing board, employees, vendors, and customers serve that purpose for organizations. Stakeholder surveys can be used as a powerful governance mechanism to assess cultural dimensions, especially when integrated into channels of communication already established between the organization and its stakeholders. Stakeholder surveys should be designed to gather

culture. Survey data must be presented in a way that is useful to make good choices about emerging risks and managing resources. For example, would an internal auditor modify his or her audit plan based on a review of the information that shows a comparative analysis between overall company and business unit ethics ratings?

Although stakeholder surveys are not new, the survey data can be transformed into cultural risk intelligence that provides leading indicators of risk. Once the internal auditor has gained confidence in the survey content, it is essential to establish a periodic checkpoint for the purposes of trending. Trending and ongoing monitoring provide an excellent source of cultural intelligence and a prudent way to identify the people-related risks on the horizon that need to be evaluated and addressed to safeguard the organization.

Internal auditors must be as wise as the board, as savvy as management, and as shrewd as attorneys.

allows internal auditors to determine whether cultural risks are being managed well. The internal auditor should examine the results of incidents reported during the period under review to determine whether sufficient information is available and appropriate responses have been made. For example, is the status of incidents tracked to determine the timeliness of review and resolution? Have incidents resulted in policy changes, organizational changes, disciplinary actions, restitution, or prosecution? Do a high percentage of incidents remain under review for an excessive amount of time, or are they quietly closed due to insufficient information? Just as an organization treats good behavior with praise, it should also know how to meet inappropriate behavior with criticism to promote the organization's value system.

Cultural Trending and Monitoring


Cultures don't erode overnight. Rather, small risks grow over time when they are ignored by a small

meaningful information about management and employee ethics, the systems for protecting informants from retaliation and encouraging the reporting of wrongdoing, and the systems for enforcing fair and uniform disciplinary actions.


The internal auditor's evaluation of the culture must go beyond just reviewing the written code and governance standards. The culture of the board and senior management drive the ethical behavior and governance practices underlying the organization's risk management and internal controls. Only the board and senior management can establish the tone at the top; however, the effectiveness of this tone can best be determined by surveying external and internal stakeholders throughout all levels of the organization.

When assessing organizational culture, the internal auditor's use of cultural surveys can leverage the value of qualitative insight with quantitative precision to measure the effect governance has on organizational

RIISING TO THE CHALLENGE

In a world where risk is infinite and resources are limited, the internal auditor still is expected to improve risk management. With a fresh focus on governance and the people-related aspects of the organization, internal auditors can provide valuable insight into emerging risks. Internal audit's role in ethics, governance, and culture may be one of the most challenging responsibilities for the profession, yet it is also the most essential for advancing organizations and society. The new era of internal auditors must become as wise as the board, as savvy as management, and as shrewd as attorneys. Most notably, internal auditors must exercise fair and ethical judgment, and must be an honest voice of reason as the conscience of the organization. 

MICHAEL BROZZETTI, CIA, CISA, CGEIT, is a principal at Boundless LLC in Philadelphia.



The dynamic, fast-paced nature of Agile software development requires auditors to think differently about internal controls.

David Tilk

5 steps to *Agile Project Success*

M

ore and more organizations have been turning to the Agile methodology for their software development efforts. According to PricewaterhouseCoopers' Global Portfolio and Programme Management Survey 2014, use of Agile has increased by 11 percent since 2012. At the same time, many internal audit functions are struggling with how to interact with Agile projects, especially those whose experience lies with more traditional, system development life-cycle (SDLC) controls.

Agile processes help project teams manage unpredictability through a focus on adaptive planning and rapid, flexible response to change. The Agile philosophy encompasses several iterative software delivery methodologies—including scrum, extreme programming, and feature-driven development—that emphasize a lean, interactive approach to product development. In fact, Agile is not confined to a single method of delivery—most organizations take a hybrid approach, drawing

from multiple iterative development methodologies. The products to which Agile is applied typically emphasize making usable code available quickly to meet business needs.

Agile project management focuses on perceived value-add processes. The values that underpin this approach, as defined by the Agile Manifesto, specify that: a) individuals and interactions are more valuable than processes and tools, b) working software is a higher priority than comprehensive documentation, c) customer collaboration is more important than contract negotiation, and d) responding to change is preferable to following a rigid plan.

Auditors familiar with traditional SDLC controls will likely recognize that some of the Agile values conflict with more established methodology. The traditional controls are typically implemented “after the fact,” and they rely heavily on documentation — neither of which works well with Agile methodologies. To help close the gap between their knowledge of traditional models and the Agile method, internal auditors should consider five steps aimed at enhancing work with Agile teams. Following this approach, practitioners can help the team, and the organization, execute its compliance responsibilities effectively while making sure not to erode the value of Agile methodologies.

1

GET INVOLVED EARLY, UNDERSTAND THE PROCESSES

The earlier internal audit gets involved, the better. Working with Agile teams in the early stages of project development increases understanding of the project’s life cycle and its key benefits, drivers, and objectives. That understanding, in turn, enables internal audit to better contribute to the project

as the team defines its risk management approach and strategy.

Before internal audit can begin scoping an Agile project, it has to understand the processes. Auditors should spend time with the process owners and ask them to explain their version of Agile. Although scrum is the most commonly used approach, auditors should never assume that scrum, or any other method, has been selected.

Numerous Agile variants exist, and some organizations even develop their own in-house methodology based on Agile’s core values. Several variants, in particular, are commonly encountered:

- **Scrum** is often used interchangeably with Agile and focuses on the project management of the product or SDLC. The methodology emphasizes collaboration, functioning software, team self-management, and the flexibility to adapt to emerging business realities. Scrum is highly collaborative, often benefiting from cohabitation of resources.
- **Extreme programming (XP)** is an Agile variant that focuses on the software engineering component of SDLC. The approach is best suited to small, focused teams and promotes simplicity of code. It features frequent releases in short development cycles, coding in pairs, and unit testing of all code.
- **Lean development** is a variant common to scrum that focuses on SDLC project management. Lean development’s roots are grounded in Lean manufacturing theories — the methodology consists of start-up, steady-state, and transition or renewal project phases.
- **Crystal methods** are a collection of various Agile-like methodologies focused on streamlined, optimized, integrated teams, with a specific method applied to each

project depending on communication requirements, system criticality, and project priority.

Other variants of Agile include hybrids such as feature-driven development, test-driven development, Waterfall-Agile, the dynamic system development model, and the Agile unified process. Internal auditors should make sure they understand the project methodology’s objectives, process controls, and documentation and process requirements before a risk management approach and strategy are defined.

2

ASSESS RISK AND CONTROL

Once the chosen methodology is understood, internal auditors should map out process control points — even if the project team doesn’t necessarily view them as controls. Two control points from the scrum methodology provide illustrative examples:

- **Product backlogs** comprise the store of all user requirements in the form of stories that communicate what the end user should be able to do, and the benefits accruing from those features. A backlog, and variations of it, exists for every Agile project and should be available to everyone involved. Documentation such as test cases and results, as well as specifications, vary from team to team. If a product backlog can’t be produced, the auditor should inquire about it with members of the Agile team.
- **Burn-up/burn-down charts** are the primary tool many teams use for tracking their progress. They measure the total in-scope work, the amount of work that should have been completed by a particular time, and the work actually completed. In effect, the charts

More than **two-thirds** of organizations are either “pure Agile” or “leaning toward Agile” for their software development, according to a 2015 HP study of development and IT professionals.

take the place of several traditional project controls and could be viewed as a type of earned value analysis. Such charts reveal where project efforts are focused, and where they should be focused, as well as help identify significant changes in scope.

Once internal auditors develop an understanding of the inbuilt controls, they should examine the project’s inherent risk profile. While Agile development can provide significant benefits to a project—such as more frequent releases of code and better alignment between users’ needs and the finished product—it also introduces risks that need to be considered and managed correctly.

The traditional roles of business users, developers, testers, and IT experts have become more cross-functional and integrated to support leaner project teams and continuous delivery. Consequently, some of the traditional control gates may not exist as expected on Agile projects, particularly with regard to segregation of duties. That’s especially true in organizations that have adopted a development operations (DevOps) strategy. DevOps sees operations and development engineers working together throughout the life cycle, from design to production support.

Auditors need to understand the project team’s approach to segregation of duties and code production, and examine controls within that approach. Agile processes should result in an increase in automation, including testing and approval, as opposed to traditional manual sign-offs. Internal audit must become familiar with those tools and processes as well as know how to interpret the outputs of automated systems and logs.

Auditors should also be mindful of the risk that Agile project iterations could become delayed by traditional

functions such as change and release management. They should assess the project team’s ability to integrate with those functions, and raise issues related to interactions with them—including the functions’ ability to support rapid-delivery models.

Documentation issues may also present a risk. While Agile-delivery methodologies by their nature seek to generate less documentation than traditionally required, that doesn’t mean documentation should not exist. Auditors should work with the team to find the minimum documentation standard

Some traditional control gates may not exist as expected on Agile projects.

acceptable and determine whether the product backlog, or an extension of it, achieves the required level of comfort while still promoting Agile principles.

Lastly, one of Agile’s biggest benefits—its short turnaround cycles—also represents one of its inherent risks. The discipline’s iterative nature can make it difficult to realize the promised business value, if the effort’s scope is continually evolving. Agile teams need to put a mechanism in place that isolates the effort while still capturing future functionality in the product backlog. That functionality should then be turned into a separate effort that can be controlled independently.

3

KNOW HOW AGILE TEAMS DEFINE DONE

One of scrum’s primary tenets states that teams following the methodology are self-organizing and self-directed, meaning that individual teams largely identify and implement their own standard practices and



quality control metrics. And because quality measures can vary from one team to the next, differing notions of what constitutes project completion may exist. Examples of the Agile team's methods for defining when a project is "done" include:

- **A code/configuration review process.** The team may require many levels of solution-level reviews to confirm adherence to design or development standards, to promote optimized and sophisticated error logging and error handling, or to meet other required solution needs.
- **Testing requirements.** Different industries and their solutions may necessitate varying levels of testing standards and practices.
- **Traceability.** Many project teams apply the contents of the Agile Manifesto to promote a *document-free* process versus a *documentation-driven* process. However, a well-practiced Agile team can, for example, provide traceability that links working product features to requirements (user stories taken from an approved product backlog), design documentation, test evidence, and release strategy and documentation.

Understanding the team's definition of *done* leads to an entry point for a risk-based conversation about the effective use of Agile to deliver business value. The definition serves as a quality control mechanism, though it also acts to promote adherence to practices aimed at reducing risks associated with Agile development.



ASSEMBLE THE RIGHT SKILLS

Agile-based projects feature unique risks and control structures, and understanding them

is crucial to the review process. Audit teams need to align the right expertise with planning and review activities, enabling practitioners to:

- Ensure a sound understanding of the problems and risks.
- Establish credibility and confidence in the program team.
- Build empathy with the delivery team.
- Deliver practical, meaningful insight to the project team.
- Provide actionable feedback that promotes more effective use of Agile without introducing additional business risk.

Subject matter specialists with experience in both delivering and reviewing similar projects are also key to successful reviews. Specifically, auditors reviewing Agile projects should have more than a basic understanding of Agile processes, familiarity with the toolset being used, an understanding of how to extract and interpret the required information, and a grasp of the path to production that is being used by the project teams.

Once the review team is in place, auditors should make sure their approach focuses on delivering value. In particular, they need to understand what the project team is trying to achieve and link audit activities to those aims. To achieve alignment, practitioners should consider an objectives-based audit program. Rather than reviewing compliance against a particular risk and issues template, for example, the team should determine whether the overall objective of "managing risks and issues effectively" has been met. Auditors may want to consider using an assessment framework that goes beyond control outcome.

Practitioners need to provide relevant, actionable, and timely feedback that will enhance the likelihood of project success. Moreover, reviews

The two leading causes of **Agile** project failures are **lack of experience** with Agile and a company culture that is at odds with Agile values, according to the Ninth Annual State of Agile Survey.

should not be limited to solution and delivery risk—practitioners may want to consider external and commercial risk and examine any corresponding mitigation strategies. These factors contribute to the likelihood of project success and may be critical to a meaningful review. Auditors should familiarize themselves with not only the expected controls outcomes of the project, but also the required technical and business outcomes, allowing for a more rounded view to be developed.

5

ESTABLISH REPORTING PARAMETERS AND PROVIDE REAL-TIME FEEDBACK

To deliver maximum value to the project

team, auditors should explain the nature of the engagement and obtain agreement up front regarding how and when they will release reports. Is the review a formal internal audit, or is it a health check or other activity aimed at performance improvement? Will the reporting be delivered through standard channels or directly to the project's governance structure? The answers to these questions guide the reporting for eventual review.

Internal audit and the business should also agree on the most efficient and practical reporting format. Agile projects run at high speed and in high-pressure environments—quite often, value can best be realized by near-real-time feedback. Timely, practical, and actionable reporting is key to Agile's success.

RELEVANCE AND VALUE

As noted in PwC's 2015 State of the Internal Audit Profession Study, internal audit functions that focus on adding value are outperforming other teams in terms of business alignment and talent models. Understanding a project's objectives, as well as the risks associated with project methodology, helps enhance the value internal audit can deliver. The key is simple: Engage with teams early, understand what they're doing, modify the approach as needed, and provide relevant feedback—all while helping the Agile teams and the organization better understand and control risk. [la](#)

DAVID TILK, CISA, PMP, is national project assurance leader at PricewaterhouseCoopers in Cleveland.



Responsive. Intuitive. Enhanced. The *Internal Auditor* Website Delivers More

Garner internal audit insight like never before with access to the current/archived content, exclusive online features, blogs, and video with optimized options to search and comment/share.

Go experience InternalAuditor.org.



2015-1636

KICK-START *Your* CAREER DEVELOPMENT PLAN



**INVEST IN YOUR FUTURE BY
INVESTING IN YOURSELF.**

Download our free guide today
www.theiia.org/professionaldevelopment

Ready to get started? Develop your
internal audit skills with IIA Training.
www.theiia.org/training



 **The Institute of
Internal Auditors**

Governance Perspectives

BY ROBERT WESTBROOKS

EDITED BY MARK BRINKLEY

U.S. GOVERNMENT STEPS UP ITS GRC GAME

New guidance provides opportunities for federal auditors.

This year is shaping up to be big for governance, risk, and control activities in U.S. federal agencies. The federal playbook has been enhanced for the coming season with an update to the Standards of Internal Control (i.e., Green Book) and new guidance from the Office of Management and Budget (OMB). Federal auditors have opportunities to add value within their organization's lines of defense in risk management and control.

The Government Accountability Office updated the Green Book in September 2014 and adopted The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control—Integrated Framework*. It is effective for federal agencies starting fiscal year 2016. State, local, and quasi-governmental entities, as well as not-for-profit organizations, may also adopt the Green Book as an alternative to other control frameworks.

The previous Green Book was issued in 1999 before the Enron, WorldCom, and Tyco accounting scandals; before the enactment of the U.S. Sarbanes-Oxley Act of 2002; and before the financial crisis of 2007–2008. These events moved risk assessment and risk management to the forefront and precipitated greater emphasis on “quality information.” The updated Green Book contains significant revisions and introduces 17 principles for management to add depth to the five components of internal control.

OMB Circular A-123 includes detailed guidelines for the evaluation of systems of internal control. The OMB is revising the circular, and a discussion draft has been disseminated to agencies for comment. The revised circular likely will be issued in fiscal year 2016 to harmonize the guidelines with the revised Green Book. In addition to emphasizing the need to manage risk and internal

control in both financial and nonfinancial areas, the new Circular A-123 is expected to require federal agencies to adopt enterprise risk management (ERM) and may simplify the annual management assurance statements required under the Federal Managers' Financial Integrity Act.

In the private sector, where ERM has taken root, uncertainty remains about how risk management and internal audit should interact so audit can add value while maintaining independence. This is more challenging in the federal environment, given the inspector general's (IG's) role. IGs conduct independent audits and investigations. They report to Congress and are under the general or nominal supervision of the agency head, who may not prevent or prohibit the IG from conducting any audit or investigation. The office of inspector general (OIG) auditors also are responsible for conducting criminal and administrative

READ MORE ON GOVERNANCE visit the “Marks on Governance” blog at InternalAuditor.org/norman-marks



TO COMMENT on this article, EMAIL the author at robert.westbrooks@theiia.org

investigations. IGs are required by law to keep Congress and the agency head fully informed and current on issues. While private sector auditors are restricted by Standard 2440: Disseminating Results in releasing audit results outside the organization, IGs are required to publicly release reports.

At the Pension Benefit Guaranty Corp. (PBGC), where I serve as IG, we are seeking ways to balance independence with positive engagement as we adopt the new Green Book and implement an ERM program, as mandated by Congress. Our office previously identified internal control deficiencies that resulted in the PBGC receiving adverse opinions on internal control. To help management, we have targeted audit work on the governance of internal control to identify gaps among the five components of internal control. We have issued risk advisories to aid in risk assessment, and we issued a white paper to help champion the establishment of an ERM program.

The “fan of activities” infographic in the 2009 IIA Position Paper, *The Role of Internal Auditing in Enterprise-wide Risk Management*, is useful with regard to audit’s role in ERM. OIG auditors don’t own risks, but at a minimum we may be relied on to give assurance on the ERM process and be asked to evaluate

the reporting of key risks. Management should use our evaluations to monitor the design or operating effectiveness of the internal control and risk management programs at a specific time or of a specific function or process. The OIG also is responsible for informing management about fraud and other risks. I have used the fan infographic to show core audit roles in regard to ERM, possible roles if safeguards are in place to protect our independence, and roles we cannot undertake. The Three Lines of Defense model also has been useful in defining and showing expectations of our respective roles and communication channels to those charged with governance.

Managers across the federal government are apprehensive about how OIG auditors will evaluate their agency’s adoption of the new Green Book and the role of OIG auditors in ERM. At the PBGC, we will fulfill our statutory responsibilities, understanding we provide the most positive engagement with management when we foster an environment where the seeds of a robust internal control framework and ERM can grow. [la](#)

ROBERT WESTBROOKS, CIA, is the inspector general for Pension Benefit Guaranty Corp. in Washington, D.C.



Engage and Connect Globally

Gain a competitive edge with unique IIA advertising and sponsorship opportunities as diverse as the 180,000 members in the 190 countries we serve.

Contact +1-407-937-1388 or sales@theiia.org for more information.

www.theiia.org/goto/advertise

 **The Institute of Internal Auditors**

2015-1635



BY J. MICHAEL JACKA

WHEN RISK MANAGEMENT FALLS SHORT

A recent film provides important lessons that all internal auditors can learn from.

The movie, *The Big Short*, based on Michael Lewis' well-researched and eye-opening book, tells an enlightening story. The book was the only source I'd found that came close to providing a cogent explanation of the housing market bubble, the impact of subprime mortgage bundling, and the subsequent recession. Within the story are several interesting lessons, including some that internal auditors should take to heart.

Details always matter.

Subprime mortgage bundles are complicated investments. In 2005, buried deep within those bundles were subprime loans of questionable value. Those who doubted the veracity of the bundles dug deep and found details most people overlooked. Auditors must do the same. The devil is in the details, and that is often where the risks lie as well.

Ask stupid questions.

The investors who bet against the bundled mortgages—and made a fortune in the process—asked the

stupid questions. Everyone else just assumed they knew how it all worked. (Or they didn't care how it all worked because they only cared that it was, indeed, working—see the next lesson.) Some of the best findings seem to come from new auditors because they are not afraid to ask the so-called stupid questions. The rest of us think we already know the answers, and we are often wrong. Auditors shouldn't worry about appearing ignorant—the stupid questions often lead to the most revealing answers. In fact, the only stupid question is the one you don't ask.

Audit success. One of the main reasons that no one investigated the bundled mortgages is that everyone was making money. During risk assessments, few people—auditors included—place a priority on reviewing areas of the business where success is being achieved. Their focus quickly turns away from these ventures, divisions, or processes. Auditors should look closely at success and determine whether or not

contingencies exist for when the success runs out. And they should make sure success is not a result of smoke, mirrors, and questionable accounting. Success does not mean that risks have been removed.

None of the foregoing is meant to implicate the internal auditors within organizations that played a part in the economic collapse. I was not in their situation, and I refuse to second guess those involved in such a complicated and devastating set of circumstances. However, it is important that every one of us looks closely at past events—what we've done, what others have done, and the ramifications of those actions—to learn how we can do our jobs better. We cannot assume everything is fine, nor can we assume everything has gone awry. What we can do is move past assumptions and into proof about the risks our organizations face. [ia](#)

J. MICHAEL JACKA, CIA, CPCU, CFE, CPA, is cofounder and chief creative pilot for Flying Pig Audit, Consulting, and Training Services in Phoenix.

READ MIKE JACKA'S BLOG visit InternalAuditor.org/mike-jacka

IN US THEY TRUST

There are specific steps internal auditors can take to build lasting relationships with their stakeholders.



MICHAEL ROSE, CIA, CCSA, CRMA, CPA, Partner, Governance, Risk, and Compliance Practice Leader for Northeast and Atlantic Coast Territories, Grant Thornton LLP



ERIC HOLT, CRMA, Global and National Partner in Charge-Internal Audit, Risk & Compliance Services, KPMG LLP

How would you define trusted adviser?

HOLT For internal audit professionals to be seen as trusted advisers, they must be viewed by all key stakeholders as having strong knowledge of the organization's key business strategies and goals. Also, to drive incremental value across the organization, they must be able to provide advice and perspective on issues beyond merely providing assurance. It takes time to build a trusted adviser relationship, and the path must start with a clear understanding of stakeholder expectations and strong, frequent collaboration with all key stakeholder groups. Without deep knowledge of the business, internal audit will not earn the trust of stakeholders, and without that trust there will be no opportunity to provide advice.

ROSE The trusted adviser is the person a stakeholder calls first when issues or crises arise. In that time of great need, the trusted adviser

is the person in whom the stakeholder has the most trust and confidence, and who will offer the best advice and assistance. Both parties benefit from this type of relationship, which empowers individuals to affect organizations in meaningful ways. The individuals in this type of relationship are comfortable and open with each other and do not let anything erode their mutual trust. The internal auditor can work to build this type of relationship through gaining knowledge of the business, setting clear expectations, bringing value to the organization outside of the normal assurance type of auditing, and collaborating with stakeholders.

Why aren't more internal auditors considered trusted advisers?

ROSE Historically, many internal auditors have worked verifying past events. Audit strategies and plans have been developed focusing on performing audits of internal

controls around processes and transactions that have already occurred. The audit process has been a compliance approach moving toward focusing on areas of highest risk. Many internal audit departments have a culture of content knowledge and technical skill alone and, in some cases, lack a deep understanding of the business, which is visible to stakeholders. There has been much focus on the daily work and alignment with budgets. The paradigm shift will be to listen first and then actively solve the problem at hand. Providing valuable advice that can be used in the business will only come with this expansion of the auditor's knowledge of the business.

HOLT The key reason is internal audit's perceived lack of in-depth knowledge of the business, which includes a thorough understanding of strategies and goals. KPMG recently teamed with *Forbes* to survey more than 400 audit committee chairs and

READ MORE ON TODAY'S BUSINESS ISSUES follow @IaMag_IIA on Twitter



TO COMMENT on this article,
EMAIL the author at editor@theiaa.org

chief financial officers regarding their perceptions of the value delivered by internal audit. One of the findings of the Seeking Value Through Internal Audit survey was that 55 percent of all respondents indicate they want their internal audit function to do more to improve its knowledge and expertise to a point where it can match the sophistication of its audit targets. Without this level of knowledge and expertise, key stakeholders will not view internal audit as having valuable input into their key issues and challenges.

How can internal auditors become trusted advisers to the audit committee and executive management?

HOLT To gain the trust of these key stakeholders, internal audit should demonstrate that it understands how these constituencies define value and what their specific expectations are of internal audit. Once these expectations are known, audit can ensure value is delivered and over time become the trusted adviser both the audit committee and executive management expect. To be effective, there must be frequent interaction between internal audit and these stakeholders to ensure changes in expectations are understood and addressed. Ongoing, consistent collaboration and effective communication are critical.

ROSE The characteristics of a trusted adviser are earning and gaining trust, building and strengthening of the relationship, listening intently to enable focus on the issue at hand, and providing advice. There must be total commitment to the process. Internal auditors should first focus on understanding what is most important to the audit committee and executive management. The result may show total alignment or disconnect, but it is important to understand the priorities of the various stakeholders. In building this trust relationship, some important initial factors are a sense of responsiveness to stakeholders' concerns, reliability, availability, and a sense of inclusion of the audit committee and executive management in findings and results discussions.

How can internal auditors overcome resistance or skepticism about their advisory efforts?

ROSE Trust is the one thing that can change a relationship. I have an example where a CAE decided he needed someone independent to interview various members of senior leadership to understand their opinions of internal audit and the value of its advisory efforts. It became clear through the interview process that the vice president of operations had the most resistance to internal audit's advisory efforts. This individual lacked an understanding of internal audit's role within the organization. Based on the interviews, it was recommended that formal meetings be scheduled with that vice president at least once a quarter to discuss various aspects of

the business and how the audit plan covered risks associated with operations. Additionally, it was suggested submitting to the vice president the audit plan initially and, in subsequent quarters, a scorecard with quadrants showing issues being addressed, new areas to be examined, and various current industry topics. Finally, I recommended earning a seat at the table to show a clear understanding of the business and industry expertise, beginning to build credibility, and developing a stronger relationship over time. Over the last year, these recommendations have helped the CAE build a relationship with the vice president, who is beginning to request internal audit's advice before undertaking system changes, addressing issues affecting the business, or entering into agreements.

HOLT It is internal audit's responsibility to educate key stakeholders about the role it should be playing with regard to operational and strategic risks. However, to establish credibility, internal audit must possess the skills to meet the expectations of each stakeholder group. Repeatedly demonstrating audit's knowledge of the business and ability to provide valuable insights and advice will eventually remove the level of resistance and skepticism regarding internal audit's advisory role.

How is the role of internal audit changing?

ROSE Organizations are operating in markets where they are being challenged by significant risks such as data privacy and security, governmental regulation/compliance, and market and consumer risks that inhibit their ability to execute their strategies. Internal audit must have the talent to understand its organization's entire business and be relevant in offering valuable insights. Some of those areas internal audit must focus on include the highest risks of executing the organization's strategy; capabilities to focus on strategy, finance, operations, and compliance; aligning with enterprise risk management and all lines of defense; use of technology tools, such as data analytics, to provide a meaningful view into the business; and talent acquisition to gain the key skills needed in this changing environment.

HOLT The role of internal audit will continue to evolve with the expectations of each of the key stakeholders. The results of the recent KPMG/*Forbes* survey indicate that expectations are growing and evolving in three key areas. First is risk management—internal audit needs to do a better job of detecting and assisting the organization in responding to emerging risks. Second is technology—internal audit must continue to evolve in its use of data and analytics to provide more effective delivery and enhanced insights. And third, value—internal audit must continue to deliver value through enhanced insights regarding assessing risks and risk management practices, providing an informed perspective on emerging risks, and focusing on sustained profit enhancements. [la](#)



BY TED DOANE

PUBLIC SECTOR INNOVATION

Adding value in government settings relies on the audit function's ability to help reinforce innovative thinking.

Status quo thinking has no place in today's public sector organizations. Much like the private sector, governments need to align their activity to a rapidly changing environment and rising stakeholder expectations. Government entities need to be more flexible, adaptive, and perhaps most of all, innovative. In turn, government auditors need to support innovation, ensuring significant risks are identified and assessed. But their approach, just like that of the organization, must adapt to changing needs.

Governments seeking to foster innovation need to build a greater tolerance for risk, and their auditors must be attuned to these efforts. Traditionally, governments have been risk averse and reluctant to expose what is not going well, hampering innovation for fear of stakeholder reprisal. The culture needs to change. For innovation to be effective, managers should build risk tolerance needs into the design of pilot programs to allow for a reasonable failure rate (e.g., 20 percent). Internal auditors need to recognize such allowances and acknowledge

when management has managed its risk effectively.

The tone of an internal audit report, or the nature of an observation, will influence how governments manage innovation-related activity. For maximum impact, internal auditors must clearly understand their stakeholders, the risk environment, and organizational objectives. The audit report's observations and recommendations will add value and improve operations if these messages take into account clients' intention to innovate.

The audit schedule also needs to reflect both the risks and opportunities of innovation, and it must be flexible and responsive to change. The schedule will support a culture of innovation as long as internal auditors work with management to examine problems and provide objective solutions. Planned engagements need to include insightful, focused objectives that address innovation, such as examining the effectiveness of an innovative practice to determine its relevance and assessing whether the activity is achieving its intended outcome.

Supporting innovation efforts also requires internal

audit to draw upon a diverse team of experienced, talented employees, with a deep understanding of government. Audit management needs to assess the objectives, scope, and intended outcomes for projects and identify the appropriate skills for the team. Outsourced or cosourced resources should be considered if specialized expertise, such as IT or actuarial experience, is required. The function also needs to have a long-term human resource plan to ensure the team's skills remain relevant.

Internal auditing is well-positioned to support an innovation agenda by providing management and the audit committee with informed, unbiased opinions. Auditors must embrace innovation, and practice it themselves, to help clients adopt innovative practices. By reinforcing innovative thinking, auditors can help government officials find the best solutions to the many complex and growing challenges facing their constituencies. [la](#)

TED DOANE, FCPA, FCA, CRMA, is executive director, Internal Audit Centre, at the Province of Nova Scotia, Canada.

READ MORE OPINIONS ON THE PROFESSION visit our Voices section at InternalAuditor.org

In 2015, U.S. companies spent over **US\$13 billion** on EPA and OSHA fines and court-ordered projects to protect public health, safety, and the environment.*



**The IIA is here to support EHS auditors in protecting their organizations.
Announcing The IIA's Environmental, Health & Safety Audit Center.**

Learn more about EHS auditing and access impactful, influential, and indispensable resources.

www.theiia.org/EHSAC

*Sources: United States Environmental Protection Agency (EPA) *Enforcement Annual Results for Fiscal Year 2015* and www.safetynewsalert.com article, "10 Largest OSHA Fines of 2015."



**Environmental
Health & Safety**
AUDIT CENTER

Accelerate Your Audit with Analytic Intelligence



IDEA 10 reveals outliers in your data

Analytic Intelligence

Analytic Intelligence immediately reveals areas of interest in your data that need investigation, helping you focus your audits and be a trusted advisor to the business. Contact us to learn more: 1-800-265-4332 Ext. 2800 or salesidea@caseware.com.

Find Out How

