Ia
INTERNAL AUDITOR

AUGUST 2016

INTERNALAUDITOR.ORG

The Cyber Resilient Organization

Confronting the Internet of Things

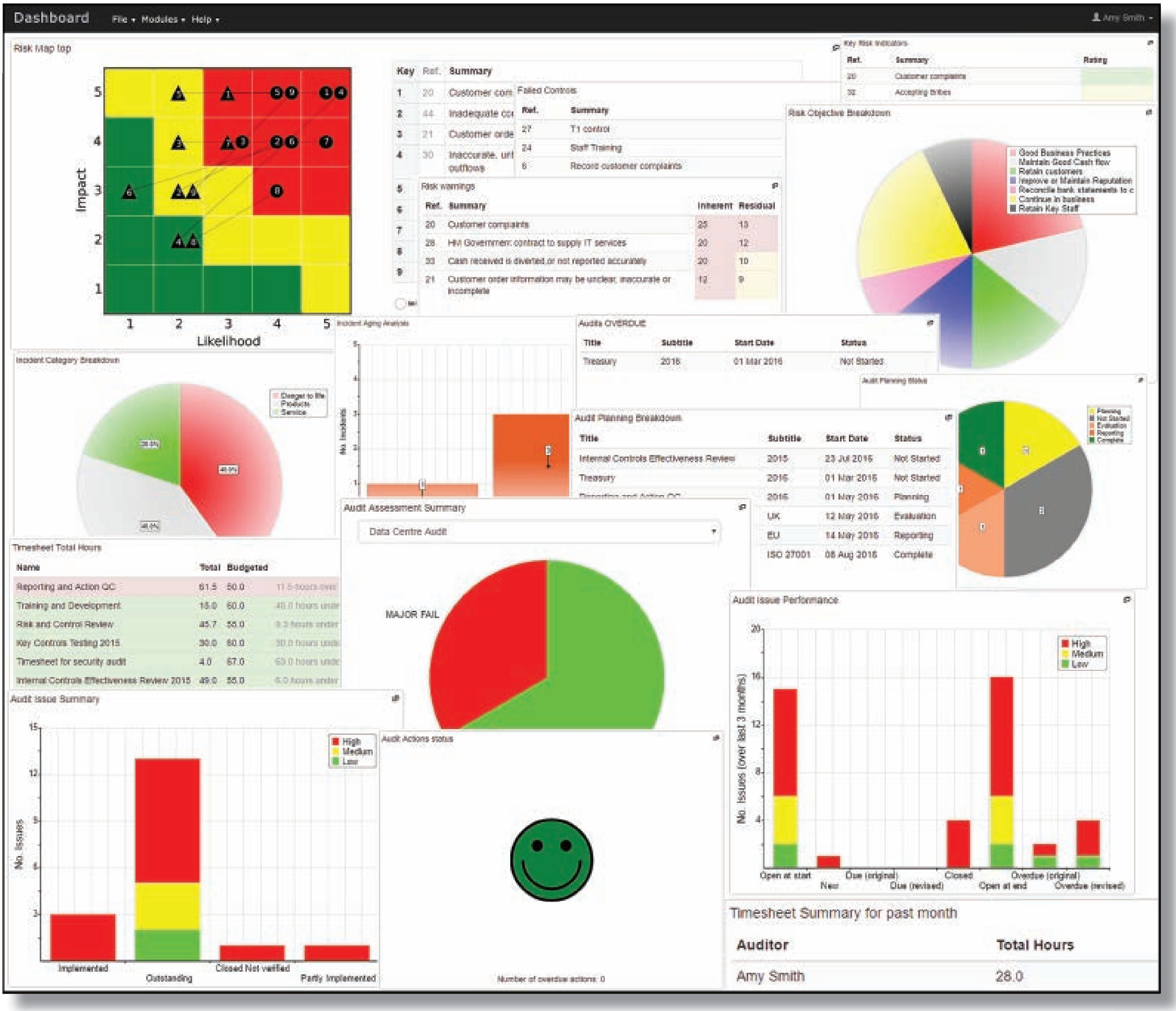
The Complex Cloud

New IIA Global Chair: Audit Never Sleeps

HYPERCONNECTED

Today's online world presents an unending array of cyberrisks.

Symbiant gives you the tools to work better



Key	Ref.	Summary
1	20	Customer com
2	44	Inadequate co
3	21	Customer orde
4	30	Inaccurate, unf outflows
5		
6		
7		
8		
9		

Failed Controls

Ref.	Summary
27	T1 control
24	Staff Training
6	Record customer complaints

Key Risk Indicators

Ref.	Summary	Rating
20	Customer complaints	
32	Accepting bribes	

Risk warnings

Ref.	Summary	Inherent	Residual
20	Customer complaints	25	13
28	HM Government contract to supply IT services	20	12
33	Cash received is diverted,or not reported accurately	20	10
21	Customer order information may be unclear, inaccurate or incomplete	12	9

Audits OVERDUE

Title	Subtitle	Start Date	Status
Treasury	2016	01 Mar 2016	Not Started

Audit Planning Breakdown

Title	Subtitle	Start Date	Status
Internal Controls Effectiveness Review	2015	23 Jul 2016	Not Started
Treasury	2016	01 Mar 2016	Not Started
Reporting and Action QC	2016	01 May 2016	Planning
	UK	12 May 2016	Evaluation
	EU	14 May 2016	Reporting
	ISO 27001	08 Aug 2016	Complete

Timesheet Total Hours

Name	Total	Budgeted	
Reporting and Action QC	61.5	50.0	11.5 hours over
Training and Development	15.0	60.0	45.0 hours unde
Risk and Control Review	45.7	55.0	9.3 hours under
Key Controls Testing 2015	30.0	60.0	30.0 hours unde
Timesheet for security audit	4.0	67.0	63.0 hours unde
Internal Controls Effectiveness Review 2015	49.0	55.0	6.0 hours under

Timesheet Summary for past month

Auditor	Total Hours
Amy Smith	28.0

"Having implemented Symbiant into our global business a year ago it has provided the complete solution we required to manage our risk and internal audit functions. It's a powerful tool, very user friendly and supported by a great team.
It's a product I would certainly recommend!"

Simon Elliott – Internal Audit & Risk – The Innovation Group Ltd

The Total Risk, Audit and Compliance Software solution

Symbiant is a modular solution that allows the whole workforce to collaborate on Risk, Audit and Compliance issues with prices starting at only $300.

Risk Registers, KRI, Incident Management, Questionnaires, Action Tracking, Audit Planning, Control Assessments, Dashboards....

To find out more or to arrange a free trial visit:

www.symbiant.us

Trusted by names you know from Charities to Banks, Government to PLC.

17 Years OF AWARD WINNING SOFTWARE

Symbiant®
Better Software

ARE YOU PART
OF THE 57%*?

Ia
INTERNAL AUDITOR

CELEBRATING 75 YEARS OF THE IIA

AUGUST 2016 VOLUME LXXIII: IV

FEATURES

TECHNOLOGY

FOR THE LATEST AUDIT-RELATED HEADLINES visit InternalAuditor.org

PHOTO ILLUSTRATION: KICHIGIN / SHUTTERSTOCK.COM;
PHOTO MANIPULATION BY SEAN YATES / YACINSKI DESIGN

Ia INTERNAL AUDITOR

CELEBRATING 75 YEARS OF THE IIA

AUGUST 2016 VOLUME LXXIII: IV

DEPARTMENTS

ONLINE InternalAuditor.org

The Opportunity of Things Boards and management are increasingly aware of the risks surrounding the Internet of Things, but are they overlooking the commercial advantages of embracing the technology?

Chairman's Video Watch The IIA's 2016-2017 global chairman, Angela Witzany, discuss her theme for the upcoming year, "Audit Never Sleeps."

Tech Know-how for Fraud Art Stewart examines the case of a credit union executive who used her knowledge of the organization's systems to embezzle funds without detection.

The Recovery Playbook Proposed NIST guidance aims to aid U.S. federal agencies in building plans to respond to cyber events.

Find us on Facebook

TOP: LEO ACADIA / THEISPOT.COM;
BOTTOM: ALI KEREM YÜCEL / ISTOCKIMAGES

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. Copyright © 2016 The Institute of Internal Auditors Inc. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Altamonte Springs, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

Editor's Note

WHAT THE FUTURE HOLDS

Technology is evolving at a breathtaking pace. Just in the past 10 years, we've seen dramatic advancements in the areas of mobile computing, wireless connectivity, cloud technology, big data, and even artificial intelligence. It's altered the way we communicate, how we purchase goods and services, and the way we do business. But where is all this heading, and what impact will it have? What changes will we see in the *next* 10 years?

Bruce Schneier, chief technology officer at Resilient, an IBM company, says in a recent *Forbes* article that we're moving toward what he calls the World-sized Web (WSW). This massive interconnected system, he says, will have two main components: sensors and actuators. The sensors will collect data, leveraging the multitude of devices connected to the web, and the actuators will affect our environment by carrying out actions. The WSW's "brains" will reside in the cloud, comprising some form of artificial intelligence. According to Schneier, the system will essentially be a "benign robot."

That's a heady concept, but perhaps not so far-fetched. In fact, the foundational components of Schneier's robot—the Internet of Things (IoT) and cloud computing—are very much a reality for today's organizations. As author Jane Seago explains in "A World of Connections" (page 28), the impact of IoT on businesses is already well underway, and it's an area that calls for close monitoring by internal auditors. She points to the abundance of connections that comprise IoT as a source of both potential benefits and great risk—working with management on both fronts, she says, will be key to auditors' involvement in the organization's IoT efforts.

Cloud computing, the decision-making center in Schneier's WSW model, is the subject of "Auditing the Cloud" on page 43. "With cloud computing becoming mainstream," the authors say, "internal auditors need to devise new ways of pinpointing the risks these services pose and verifying the security ... of critical data housed by an outside provider." They examine the many challenges presented by cloud platforms and outline key areas auditors should consider in their assessments.

Most likely, the risks and challenges associated with cloud computing, as well as IoT and other emerging technologies, will only continue to grow in the coming years. And while the shifts thus far may be substantial, and their implications for organizations vast, what's to come may be truly seismic. Schneier says the impending technology will be increasingly powerful and eventually capable of autonomy. Acting on behalf of users, it will help maximize profits but also "empower criminals and hackers."

Regardless of whether this prediction ultimately comes to pass, it's a reminder of the need to constantly look ahead and consider how emerging technology may impact the organization. To paraphrase Schneier, whatever all of this means, we don't want it to take us by surprise.

David Salierno

David Salierno

Reader Forum

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

Trusted Adviser

Good relationships with stakeholders, understanding challenges and risks, and having technical knowledge are characteristics necessary for a CAE to be called a trusted adviser. However, the same characteristics also are required for any executive-level position in the organization to deserve the title of trusted adviser.

The additional — and biggest — difficulty facing internal audit departments is having too many stakeholders to interact with. Not all stakeholders interact with each other, but the internal audit team interacts with all stakeholders. In fact, because every culture has different levels of risk aversion and acceptance for constructive criticism, even the application of our International Professional Practices Framework becomes more difficult, depending on which country the internal audit team works in, and what level of corporate governance is possible there.

YAMAN CAKIROGLU *comments on the Chambers on the Profession blog post, "Forensic Examination May Explain Why You Aren't a Trusted Advisor."*

The Fire Drill

The explanation Michael gave about how we can all learn from the fire marshall's plan execution with regard to the big picture was very accurate.

Although the article was a "Back to Basics" lesson, it is something I am trying to execute as I move forward in my career. I am a recent college graduate entering the internal audit profession, so articles like these help me hone in on the foundation of what internal auditing is all about. The impact internal auditors have can create real results if we plan effectively. Sometimes we just have to remind ourselves, as you put it, that "This is not a drill."

JESSICA HARSARAN *comments on Michael Marcucci's "The Fire Drill" ("Back to Basics," June 2016).*

Thinking Different

I don't think I can agree that Steve Jobs would have been a good internal auditor, primarily because if he saw a problem, I don't think he could help from stepping in and trying to fix it himself. As for what we can learn from him, I think one thing in particular is to "think different," which he actually used in an Apple marketing campaign. As auditors, we can get stuck in ruts or focus on certain solutions, but if we can take a step back and look at the problem differently, we might be able to suggest a better solution. Thinking differently also can open the doors to much more collaborative work.

SETH PETERSON *comments on Derrick Li's Emerging Leaders blog post, "What Can Internal Audit Learn From Steve Jobs?"*

Ia
INTERNAL AUDITOR
AUGUST 2016
VOLUME LXXIII:IV

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

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

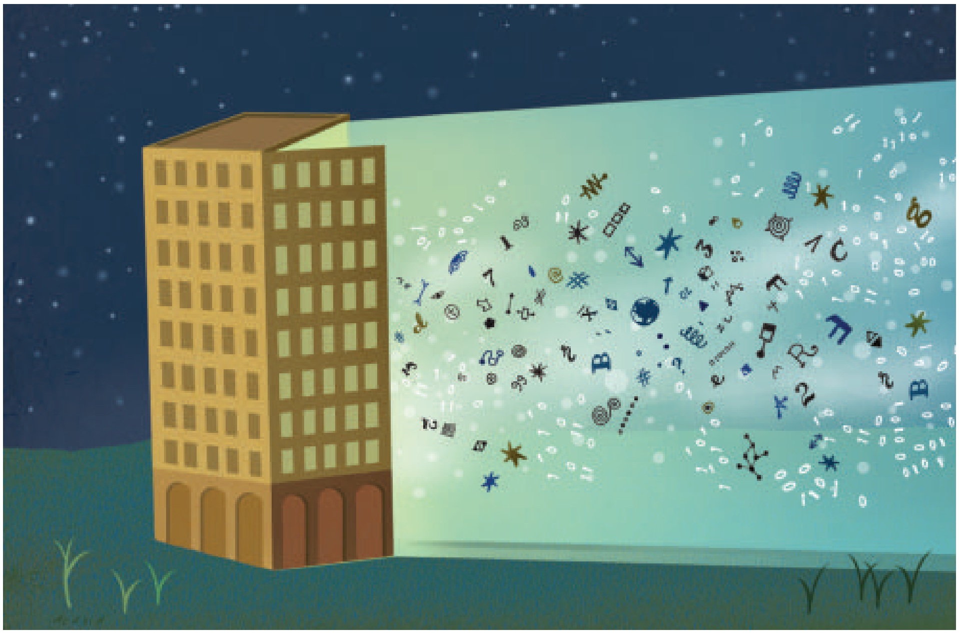
EDITORIAL
David Salierno, david.salierno@theiia.org
+1-407-937-1233; fax +1-407-937-1101

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

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

Ethical pressures hinder workplaces... Draft COSO ERM framework out... Local government innovates... Cross-industry fraud has growing impact.

Update



CYBER EXPOSED

The best prepared are getting better, but most aren't equipped for incidents.

Three-fourths of respondents say their organization's lack of cybersecurity capabilities exposes them to significant cyberrisk, reports the RSA Cybersecurity Poverty Index, based on a survey of 878 respondents from 81 countries. And although cyber resiliency has become the focus of many organizations, just one-fourth of respondents rate their organization's incident response and recovery capabilities as mature. Protection abilities are more mature than detection and response.

"We need to change the way we are thinking about security to focus on more than just prevention—to develop a strategy that emphasizes detection and response," says Amit Yoran, president of RSA, the cybersecurity subsidiary of Bedford, Mass.-based EMC.

The survey findings show that organizations have work to do on that front, with 36 percent of respondents describing their ability to detect threats as nonexistent or ad hoc. Respondents working in organizations that have experienced more than 20 cyber incidents in the past 12 months rate their cybersecurity capabilities as more developed than other organizations. "Once organizations experience an incident that negatively impacts their operations, they strive to

WHAT HAPPENED TO TRUST?

Top reasons fewer than half of full-time workers trust their employer, boss, or co-workers.

1 EMPLOYEE COMPENSATION IS NOT FAIR.

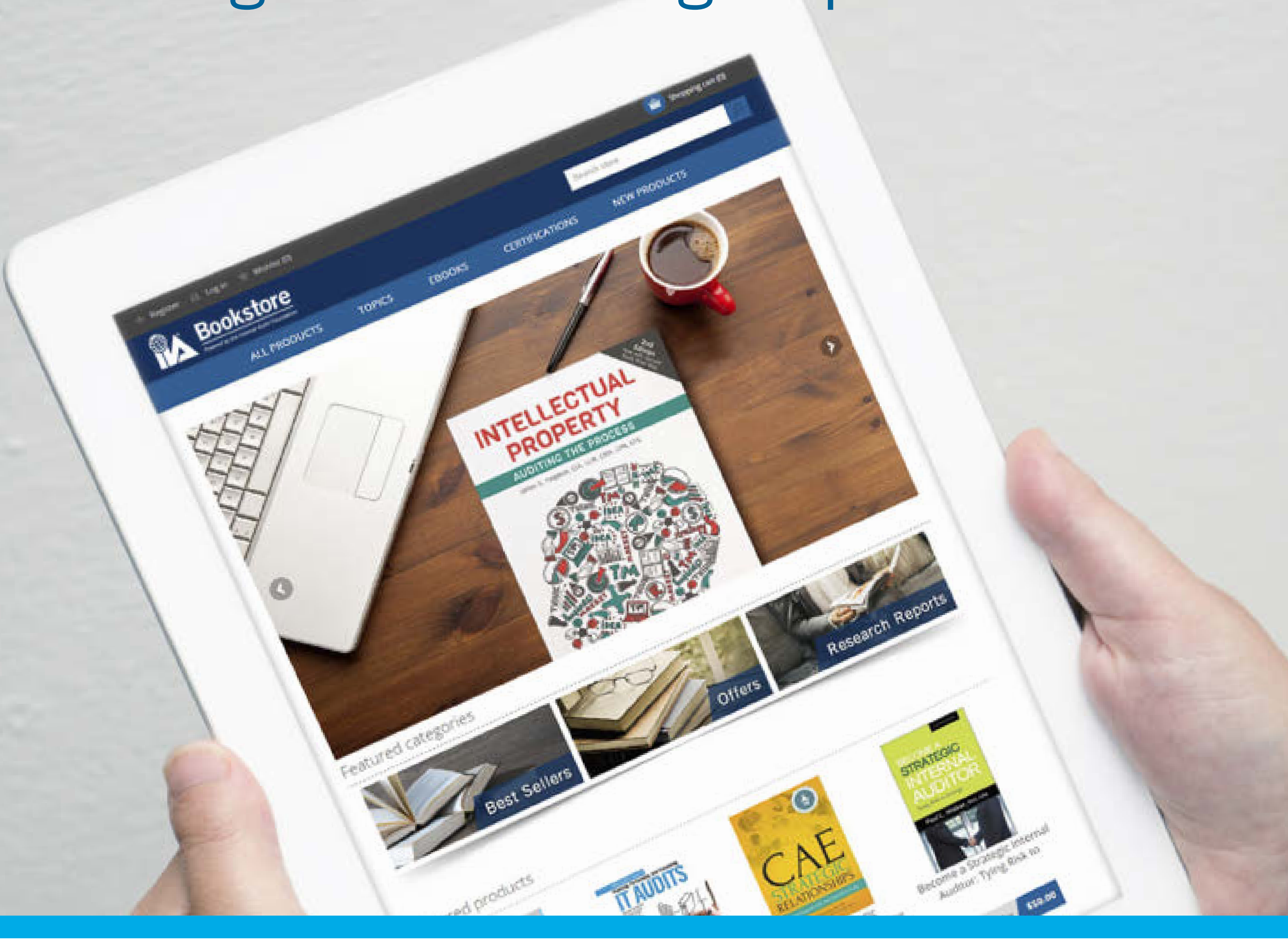
2 EMPLOYER DOES NOT PROVIDE EQUAL OPPORTUNITY FOR PAY AND PROMOTION.

3 LACK OF STRONG LEADERSHIP.

4 TOO MUCH EMPLOYEE TURNOVER.

Source: EY, Global Generations 3.0

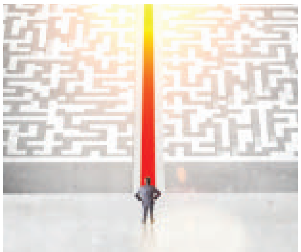
IMAGES: LEFT, LEO ACADIA / THEISPOT.COM; RIGHT, FILE404 / SHUTTERSTOCK.COM


Bookstore
ALL PRODUCTS
TOPICS
EBOOKS
CERTIFICATIONS
NEW PRODUCTS
INTELLECTUAL PROPERTY
AUDITING THE PROCESS
Featured categories
Best Sellers
Offers
Research Reports
IT AUDITS
CAE
STRATEGIC RELATIONSHIPS
STRATEGIC INTERNAL AUDITOR

improve their capabilities and maturity at a greater pace to mitigate the effects of future incidents," the index report notes.

Cataloging, assessing, and mitigating cyberrisk is the least-developed capability, according to the index. Just 24 percent of respondents rate their organization as mature in this area, while 45 percent say these capabilities are nonexistent or ad hoc in their organization. "The inability to assess cyberrisk and calculate cyberrisk appetite makes it impossible to prioritize areas of mitigation and investment," the report observes.

Although the percentage of organizations with underdeveloped cybersecurity capabilities remains constant from last year's survey, the percentage of respondents rating their organization's capabilities as "advantaged"—the highest level of maturity—grew from 4.9 percent in 2015 to 7.4 percent this year. Eighteen percent describe their capabilities as "developed," the middle level. **—T. MCCOLLUM**



48%

of employees rank productivity as their top concern.

17%

rank security as their top concern.

69%

of employees admit to sharing sensitive information outside their organization.

"As organizations continue to push their workforces to increase productivity and raise efficiency, it's not surprising that so many employees confess to taking short-cuts," says Vishal Gupta, CEO, Selcore.

Source: Selcore's Citrix Synergy 2016 survey

WORKPLACE INTEGRITY

Ethical pressure is greater during organizational change.

One-third of workers have observed misconduct in their workplace in the past 12 months, according to the Ethics & Compliance Initiative's Global Business Ethics Survey of more than 13,000 employees in 13 countries. Despite global discussions about "doing the right thing," many organizations do not know what causes people to "do the wrong thing," the report notes.

Pressure to compromise standards and observed misconduct are most common in organizations undergoing major changes. The report suggests using organizational changes as an opportunity to educate employees about the organization's values and code of conduct.

High rates of reporting misconduct correspond with more widespread retaliation against reporting, the report finds. It advises organizations to "reach out to whistleblowers during the first three weeks after a report is filed," when respondents reported experiencing retaliation. **—NICOLE LICOURT**

COSO DRAFTS ERM FRAMEWORK

Long-awaited revision addresses changes in business environment and risk.

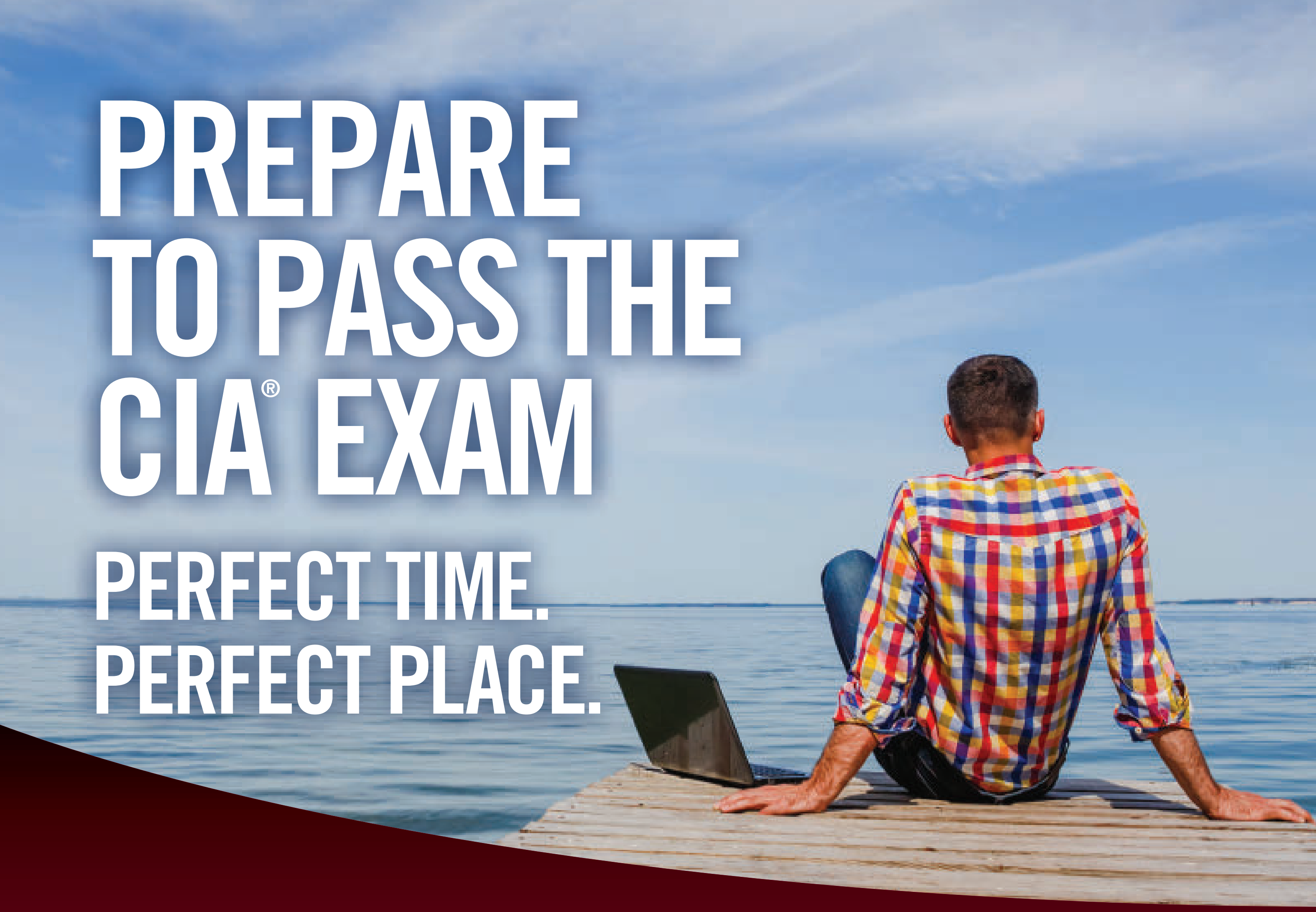
The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) enterprise risk management (ERM) framework is getting its first update since it was enacted in 2004. The recently issued draft update, *Enterprise Risk Management–Aligning Risk With Strategy and Performance*, addresses organizations' need to improve their approach to managing new and existing risks as a way to help create, preserve, sustain, and realize value. COSO is accepting public comments on its website through Sept. 30, 2016, with a final version expected in 2017.

"As we've seen the framework applied in practice, we've recognized that it has the potential to be used more extensively," says

MORE

VISIT our mobile app + InternalAuditor.org to view a video discussion of the COSO ERM draft update.

IMAGES: LEFT, RAWPIXEL.COM / SHUTTERSTOCK.COM; RIGHT, IMAGEFLOW / SHUTTERSTOCK.COM



PREPARE TO PASS THE CIA® EXAM

PERFECT TIME. PERFECT PLACE.

August is the perfect time to start your CIA and save up to US$379!

During August, The IIA is making it even easier to get started on your CIA certification. Take advantage of these two limited-time offers.

CIA EXAM APPLICATION FEE WAIVER SAVE UP TO US$200	+	THE IIA'S CIA LEARNING SYSTEM® SAVE 20%

IIA members save an additional US$100 on The IIA's CIA Learning System with member pricing.

Take advantage of August savings now!

Choose your perfect place to study with flexible study options.

Do you prefer to study on your own, when and where your schedule allows? Or do you prefer the extra guidance and structure of a live or virtual classroom? The IIA's CIA Learning System offers mobile-optimized self-study tools and facilitator-led CIA review courses. The choice is yours!

For complete details, visit
www.LearnCIA.com/august

75 ANNIVERSARY 1941-2016

The Institute of Internal Auditors

2016-2448

MORE **VISIT http://bit.ly/2adXntb to read an extended interview with Dan Hoffman.**

COSO's chairman, Robert Hirth Jr. "We realized that certain aspects would benefit from more depth and clarity, as well as greater insight into the links between strategy, risk, and performance."

With the growing complexity and speed of risk over the past decade, one of the most significant enhancements in the update is the introduction of components and supporting principles that reflect the evolution of risk management thinking and practices. It also reflects the importance of the strategy-performance connection, offers perspective on current and evolving concepts and applications of ERM, and updates the core definitions of *risk* and *ERM*.

PricewaterhouseCoopers (PwC), author of the 2004 framework, is leading the update under the direction of the COSO board and with input from an advisory council representing businesses, academia, government, and nonprofit organizations. As Dennis Chesley, PwC's Global Risk Consulting leader and lead partner for the COSO ERM update, explains, "This update more clearly connects [ERM] with a multitude of stakeholder expectations, establishes the relationship between risk and strategy, positions risk in the context of an organization's performance, and helps organizations anticipate so they can get ahead of risk and embrace the mind-set of resilience." **—S. STEFFEE**

DRIVING INNOVATION

The Internet of Things may change the way governments operate, says Dan Hoffman, chief innovation officer for the Innovation Program in Montgomery Co., Md.

You deploy first-of-a-kind technology to improve the quality of life for county residents. How do you balance innovation with managing risk? We apply three criteria to all of our projects. First, it has to be a concept or technology that we can test out in a lean, iterative manner. This helps minimize risk and limit up-front investment. Second, it has to have the potential to scale up. We get a lot of ideas that are too far-fetched. Finally, it has to be somewhat experimental. If we only went after the safe bets, we'd never be innovative.

How are the challenges and opportunities associated with the Internet of Things (IoT) different from the way you've addressed previous technologies? Some new ideas and technologies can be tested in a bubble. IoT is different. It will literally change every aspect of the way we deliver services and govern. Because of that, it's going to take a comprehensive, strategic approach. It turns our buses into roving data collectors. It eliminates entire labor categories. It changes the way we deploy first responders. So it has to be something we look at from a systems perspective so that we understand the ripple effects of each mini-revolution IoT sets off in each department.

FRAUD IMPACT FELT ACROSS INDUSTRIES

Experts point to fraud's reach beyond their immediate sector.

Nearly 85 percent of U.S. fraud mitigation professionals say fraud cases they investigate are connected to an industry outside of the one in which they work, according to the 2016 LexisNexis Fraud Mitigation Study. More than half of these cases cause an extreme impact.

The report's authors surveyed 800 fraud professionals across several industries: insurance, retail, financial services, health care, government, and communications. More than one-fourth of the respondents say cross-industry fraud is having a greater impact at their organization than within-industry fraud. Nearly two-thirds say cross-industry fraud is creating at least an equal impact.

"A quarter of professionals say they see cross-industry fraud in over half of their cases," says Bill Madison, CEO, Insurance, LexisNexis Risk Solutions.

Respondents who work in the insurance industry observe the most cross-industry fraud and say it affects their own investigations the most, especially compared to government and health care. **—D. SALIERNO**

PHOTO: RIGHT, MANX IN THE WORLD / ISTOCKPHOTO.COM

Back to Basics

BY NEHA PANSARI EDITED BY JAMES ROTH + LAURA SOILEAU

ANALYTICS-DRIVEN AUDITS

Before tackling data analytics, internal auditors need to understand the types of data, how it is stored, and how to apply it.

Data continues to be captured and processed at phenomenal rates. In fact, Computer Sciences Corp. predicts that by 2020, data production will be 44 times greater than it was in 2009. With so much data being generated, there is a need to connect the dots and get meaningful information from it. An audit that is intuitive-based and uses a selection of random samples may not be that effective in the changing business landscape. With so many automated processes, the way internal audit departments conduct audits also needs to be automated.

An analytics-based approach to audit makes it possible to review large data sets and get meaningful insights into internal control processes, including probable vulnerabilities in meeting the overall assurance objectives. The use of analytics can increase audit efficiency and lead to a deeper understanding of the business, risk assessment, and real-time monitoring. Data analysis can be applied to areas such as audit planning, sample selection, risk assessment, control testing, and identifying red flags.

Data Types and Storage

Before embracing data analytics, it is important to understand the types of data being generated. The analytics methods and tools used will depend on the type of data and the manner in which the data is generated and stored.

Qualitative data is a categorical measurement expressed with a natural language description. In statistics, it is often used interchangeably with categorical data (e.g., favorite color = "blue" or height = "tall"). Data are classified as *nominal* if there is no natural order between the categories (e.g., eye color), or *ordinal* if an ordering exists (e.g., exam results).

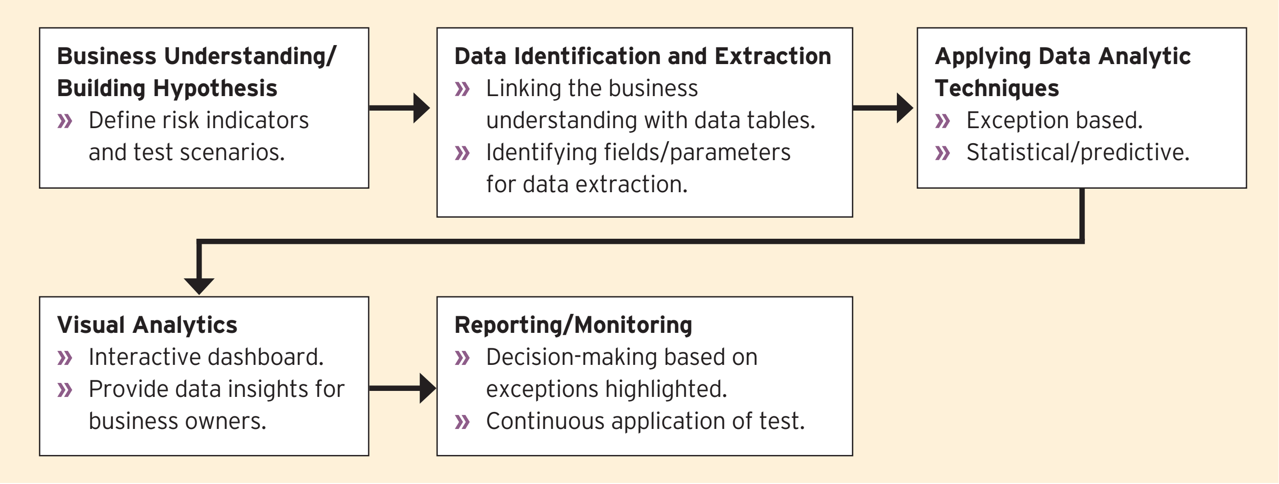
Quantitative or numerical data are counts or measurements. The data are said to be *discrete* if the measurements are integers (e.g., number of people in a household) and *continuous* if the measurements can take on any value, usually within some range (e.g., weight). Quantities whose value differ from one observation to another are called *variables* (e.g., the height and shoe size of every person are different).

Generated data is stored in data warehouses in different formats. Structured data is information, usually displayed in columns and rows, that can easily be ordered and processed. This could be visualized as a perfectly organized filing cabinet where everything is identified, labeled, and easy to access. Unstructured data has no identifiable internal structure. Types of unstructured data include word processing files, PDF files, digital images, video, audio, and social media posts.

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

TO COMMENT on this article,
EMAIL the author at neha.pansari@theiia.org

THE PROCESS OF DATA ANALYTICS



Business Understanding/ Building Hypothesis
- Define risk indicators and test scenarios.

Data Identification and Extraction
- Linking the business understanding with data tables.
- Identifying fields/parameters for data extraction.

Applying Data Analytic Techniques
- Exception based.
- Statistical/predictive.

Visual Analytics
- Interactive dashboard.
- Provide data insights for business owners.

Reporting/Monitoring
- Decision-making based on exceptions highlighted.
- Continuous application of test.

Data Analytics

Data analytics is an analytical process by which insights are generated from operational, financial, and other forms of electronic data internal or external to the organization that communicates exceptions and outliers. Exceptions are deviations from any defined criteria internal or external to the organization. Outliers are considered any data or records that are inconsistent with the population to which it belongs. Analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance.

Data analytics tools and techniques assist in transforming and improving audit approaches in terms of providing insights, predicting outcome, optimizing sampling decisions, extending audit coverage, and highlighting key deficiencies. Analytics embeds data visualization to effectively communicate insight.

Analytics is not just about technology. It refers to the use of certain technologies, skill sets, and processes for the exploration, evaluation, and investigation of data generated during business operations (See “The Process of Data Analytics” on this page).

Analytical Techniques

Analytical techniques can be used for risk assessment and control testing in various areas. It is important to link the business understanding, processes, and regulations and co-relate them with the data available to identify exceptions or outliers. There are four types of analytical stages.

Descriptive analytics identifies events that occurred in the past, while *diagnostic* analytics looks for reasons past events occurred. *Predictive* analytics predicts future outcomes based on past events, and *prescriptive* analytics provides a feasible line of action. Auditors need to gradually move from identifying what went wrong to forecasting what may go wrong. The shift from descriptive to predictive and then to prescriptive analytics requires the application of business insights with analytical techniques supported by technology advancements.

Analytics Software

Some of the numerous tools available for carrying out data analytics require coding or scripting and may not be as user-friendly compared to tools with an easy-to-use graphical user interface. Questions that can help determine which tool to invest in include: What problem needs to be solved? What are the net costs for learning a new tool? What are the other available tools and how do these relate to commonly used tools?

Changed Business Environment

Considering the ever-increasing nature of digitization, it is inevitable that internal auditors change their approach to executing audits. Traditional methods of vouching and verification may need to be reviewed to bring them in line with the changed business environment. Considering increased expectations from stakeholders and the need to look deeper into business transactions, embedding analytics in audit is unavoidable. The proliferation of new forms of data and evolving concepts of analytics-driven audits means internal auditors can gain deeper insights into the business.

NEHA PANSARI, CA, CS, *is chief manager, internal audit, at ICICI Bank in Mumbai, India.*

BY SHARIF A. NOGOD EDITED BY STEVE MAR

THE MIND OF A CREDIT CARD HACKER

Understanding how hackers work can enable auditors to focus their efforts to protect organizational data.

One of the biggest credit card fraud rings was a collaboration between Miami hacker Albert Gonzalez and hackers in Russia. The ring used SQL injection to steal more than 90 million credit and debit card numbers from retailers such as Barnes & Noble, BJ's Wholesale Club, Boston Market, OfficeMax, and TJX—the parent company of Marshalls and T.J. Maxx. Gonzalez and his crew were active for two years, and he was known to brag that he had to count hundreds of thousands of dollars by hand when his money-counting machine broke.

Gonzalez got greedy, and his flashy lifestyle caught the attention of law enforcement officials. In 2010, a U.S. federal District Court sentenced him to 20 years in a federal prison and fined him US$25,000.

Smart hackers keep a low profile and cover their tracks so they can continue the cycle. With the right campaign, they can obtain thousands of credit card numbers and sell them for millions of dollars. To help defend their organizations, internal auditors need to know why hackers target the business' credit card information, how they can steal it, and what happens after the data is stolen. That means learning to think like a hacker.

First, They Need a Vector

A vector is a network, email, application, or host that delivers a viral payload to the user. To gain entry to an organization's systems, hackers use tools, programming experience, and social engineering skills to target a user's computer or convince that person to voluntarily give them information or access. The vector they choose determines the steps they need to steal an organization's data.

Phishing is one of the more common methods. Hackers send emails to unsuspecting victims and convince them that they need to enter private information on a fraudulent website form. For example, the hacker uses PayPal's logo and a similar domain name to trick users into typing their PayPal user name and password. Internet usage policies should instruct employees to always type the name of the official website in a browser instead of clicking random links embedded in an email.

A recent variation on phishing attacks is to send employees emails claiming to be from their organization's CEO and directing them to complete a transaction.

Collect the Stolen Data

Attackers use zero-day viruses to gain access to a computer. Zero-day viruses have not been previously detected by antivirus software companies, so the software doesn't recognize them. For this reason, a

SEND ITAUDIT ARTICLE IDEAS to Steve Mar at steve_mar2003@msn.com

TO COMMENT on this article, EMAIL the author at sharif.nogod@theiia.org

hacker can quickly collect data and transfer it to his or her private server.

Speed is also essential for hackers who use phishing emails. As soon as email recipients detect that the email and site are fraudulent, it's only a matter of time before the emails are blocked and the host terminates the hacker's account. The hacker needs to collect the data from the server and transfer it to a safe location.

During the data collection stage, hackers also need to cover their tracks. They can do this by using a different host for the next vector, changing malware signatures, and setting up new anonymous email accounts.

Verify the Cards Are Valid

This step is the most crucial and risky. The hacker needs to verify the cards are valid. The hacker can do this by creating accounts at websites that sell low-priced items and don't have as much security regarding billing and shipping addresses. A list of these sites can be found through a criminal network or a search engine. The hacker makes small purchases from these online stores to verify the card is still valid and the original cardholder isn't paying attention to purchases on it.

Consumers who check their debit and credit card activity frequently can detect these transactions quickly before the charges finalize. Moreover, many financial institutions have fraud detection that automatically flags a card for suspicious transactions. These card numbers won't work, which reduces the hacker's credibility and trustworthiness with buyers.

Auditors should review security measures annually, and preferably more frequently, as risks evolve.

Because the hacker's purchases are small amounts, they can more easily slip through detection. For example, the attacker might charge US$5 on a card and wait a few days. If the charges go through and the product is shipped, he or she can make larger charges or sell the card number on the black market.

Create Fake Cards

For US$100, hackers can create fake credit cards. The number printed on the front of the card is usually fake, but the card number on the magnetic strip is one of the stolen numbers. The attacker also can sell these physical cards, but it's much more work to send the cards to a buyer.

How Auditors Can Respond

By understanding the way hackers work, internal auditors can gain better insight into ways to protect the personal data their organization has stored. Here are recommendations auditors can provide to help their organizations shore up their defenses.

System Requirements Auditors should advise the IT department or process owners to install and maintain a firewall configuration that is capable of protecting cardholder data. The organization should encrypt transmission of cardholder data across open, public networks, including wireless networks. Also, the organization should use up-to-date antivirus software and ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs. In addition, it should monitor all access to network resources and cardholder data, and test security systems and processes regularly.

Access Control Internal auditors should advise the IT department to limit access to computing resources and cardholder information only to those individuals whose jobs require it. The organization should physically secure all paper and electronic media that contain cardholder data, including computers, networking and communications hardware, paper receipts, reports, and faxes. Moreover, it should use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

Becoming a Harder Target

As their organization's third line of defense, internal audit's assurance and advisory services can be vital to protecting the business from today's hackers. Auditors should review the organization's security measures and related controls at least annually, and preferably more frequently, as risks evolve. They also can advise their organizations about ways to strengthen those measures and be better prepared to respond to an incident. With organized hackers targeting organizations from all sides, such actions can help make the difference between becoming a harder target for attackers and suffering a heavy loss from a data breach. Ia

SHARIF A. NOGOD, CFE, *is an internal auditor at Zamil Industrial Investments Co. in Dammam, Saudi Arabia.*

Risk Watch

BY ELLEN CAYA EDITED BY PAUL SOBEL

MAKE THE MOST OF ASSURANCE

Assurance maps can enable internal audit to team with other assurance providers to visually convey how risk is managed.

Most internal audit functions perform comprehensive risk assessments and quickly see there are more audits to conduct than they have the resources to execute. One way internal audit can maximize the assurance around the risks its organization faces is by leveraging the results provided by the assurance activities in the three lines of defense—line management, oversight functions, and independent assurance providers—and depicting these results in an assurance map.

Assurance mapping visually demonstrates how assurance activities apply to a specific risk within an organization. A typical map is two-dimensional, with key risks on one axis and assurance activities on another. In addition to internal audit, the assurance activities typically involve management or functional areas that review, audit, or assess key organizational risks.

Mapping Has Advantages

Creating an assurance map provides many benefits to an organization, beginning with providing the board and senior management a clear view of the organization's risks. Inconsistent or incomplete reporting makes it difficult for the board and management to execute their risk oversight responsibilities effectively. There often is not a single, comprehensive view of the key risks facing the organization and how these risks are being managed. Assurance mapping demonstrates to the board and senior management how key risks are managed because the map categorizes and assesses the assurance processes.

Another benefit of assurance maps is the ability to spot gaps in risk coverage. With so many lines of defense, it is natural that different assurance functions may believe someone else is looking at the risk. For example, risk management and compliance functions (second line of defense) are established to ensure the first line of defense (day-to-day operators who execute controls) is designed appropriately, in place, and operating as intended. However, the map may show that neither line is monitoring or managing the risk.

Assurance maps also can reduce duplication of risk monitoring activities. Many times, risk functions do not collaborate or communicate sufficiently with others. This duplication can increase costs and lead to business fatigue, as the business has to deal with multiple uncoordinated interactions among various assurance functions. Risk management and compliance functions' responsibilities may overlap with independent and objective assessors (third line of defense) who provide assurance over managing risks.

Streamlined and cost-effective assurance results from the ability to team with

VISIT http://bit.ly/29R8kvn to view an example of an assurance map.

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

TO COMMENT on this article,
EMAIL the author at ellen.caya@theiia.org

other assurance providers to determine the best way to provide assurance over a risk.

Assurance maps can enhance audit committee understanding of internal audit's assurance role, as well. This understanding can enable committee members to provide better direction on key risks they believe internal audit should be covering.

Clarity and Reliability Challenges

There are many challenges to creating a clear, concise, and easily understood assurance map. Some organizations make the map so detailed and complex that it does not give a good picture of the risks or the assurance activities being performed. To alleviate this problem, organizations should start with a specific set of risks identified through internal audit's risk assessment process, a risk management function, or even within compliance. This helps narrow the population of risks to a manageable set.

The reliability of assurance information is another challenge. While other assurance activities may not follow the same approach as internal audit, they can perform sound work around ensuring compliance, operating effectiveness and efficiency, safeguarding of assets, appropriate financial reporting, and other important controls. However, relying too much on another functional area's work, without understanding the nature and extent of the work and level of effort, can lead to poor conclusions as to how well the risk is being managed or monitored.

Internal audit can gain this understanding by assessing the strength of the assurance activities performed by the first and second lines of defense. Was the work comprehensive? Was it performed timely and objectively? Is the assurance contingent on any remediation efforts to improve the management of the risk?

Map Making

So how does an organization go about developing an assurance map? Here are some steps to get started:

1. Determine whether internal audit, risk management, or some other function will develop the map and coordinate the information obtained through collaboration among the assurance functions.
2. Identify the key risks the organization would like to map. Gain agreement from management on the completeness of the list.
3. Understand who owns each of these risks and is responsible for managing them to an acceptable level. Listing the key owner provides accountability.
4. Define a methodology and template for mapping coverage based on the organization's risk appetite and risk management framework. Map risks to processes and controls performed by day-to-day operators, oversight functions accountable for management assurance, and independent assurance providers. This will take some time to find out because there may not be one place in the organization that readily lists this information.
5. Liaise with the organization's other assurance providers and determine whether the assurance activities around these first and second lines of defense are effective. Which controls have been tested and to what extent? How do the assurance providers perform their assurance activities, and are these activities comprehensive? Does the line of defense have adequate skills to discharge its responsibilities? To help with this assessment, internal audit should leverage any audits previously performed over programs or activities of these assurance providers. Auditors also should determine when these assurance activities were last performed and whether that timing is reasonable. For example, a review of critical cybersecurity controls may not be effective if it was performed too far in the past.
6. Validate the risk coverage map with key stakeholders and clarify roles and responsibilities.
7. Decide how much assurance coverage the board and senior management require. For some risks, such as noncompliance with regulatory requirements, the organization's risk appetite might be low.
8. Implement a plan to optimize risk management coverage. This could include streamlining and optimizing controls, removing duplication in the second and third lines of defense, or suggesting additional assurance activities.
9. Develop an integrated view for executive management and the board that aggregates results from all management and independent assurance providers for each significant risk area.
10. Regularly review, monitor, and update the assurance map to ensure it remains current.

Audit Also Benefits

The need for organizations to have a comprehensive summary of the assurance that is obtained for each risk is greater than ever. Creating an assurance map can use the information supplied by internal audit and other assurance providers to understand and provide a basis on which to formulate this overall view of risk. Moreover, internal audit stands to benefit from this road map by gaining a way to determine how to direct its resources most effectively to address risk. Ia

ELLEN CAYA, CPA, *has been a CAE at Walgreens Boots Alliance, OfficeMax/Office Depot, and Excelon in Chicago.*

Fraud Findings

BY JENELL WEST EDITED BY BRYANT RICHARDS

TOUGH CONSEQUENCES

Adequate contract administration can save organizations a tremendous amount of grief and money.

Hillside Acres had a thriving parks and recreation department that offered a variety of services to its citizens. Included in these services was a community center that contained an ice rink, fitness center, and gymnasium. The city never tracked the profitability of the center, but the department typically recognized a yearly loss of US$400,000. Eventually, Hillside Acres decided to turn over day-to-day operations of the community center to ABC Co., a local, for-profit entity.

A rigorous contract was drafted that included a profit-sharing agreement; a right-to-audit clause; and clearly defined expectations of ABC when it came to accounting records, budgets, employing staff, payment of utilities, and assigning the agreement to another party with the city's consent.

Six months after the contract was issued, the local newspaper published an article about the successful public-private partnership, indicating that ABC achieved its operating goals, installed new ice at the rink, reinstated recreation programs, and enhanced senior citizen programs. Just four months later, ABC assigned its contract with Hillside Acres to CBA Co. without the city's knowledge or consent. Hillside Acres was never able to definitively identify all of ABC's owners, but it appeared that some of them also were owners of CBA.

The contract was in effect for a year before Hillside Acres realized it had not received a proposed fiscal budget from CBA. This discovery prompted an internal investigation into CBA and its operation of the community center. Complaints from vendors and employees about unpaid bills began to trickle in. The city then realized that it had been a year since ABC or CBA had provided financial statements. The city demanded those documents, along with payment of overdue bills to vendors and employees.

When some financial information was finally provided to Hillside Acres, it was not in accordance with U.S. generally accepted accounting principles (GAAP), the format agreed on in the contract. Hillside Acres brought in an independent accountant to meet with the vendor and gather the contractual information.

When the accountants requested a copy of the financial statements, CBA indicated it was unfamiliar with GAAP. Its accounting records were maintained by a bartender with no accounting training. CBA was completely unfamiliar with the concept of accrual-basis accounting and had limited accounting records for the months it was operating the community center.

The city's accountants requested a copy of the bank statements and the bookkeeping records from ABC

SEND FRAUD FINDINGS ARTICLE IDEAS to Bryant Richards at bryant_richards@yahoo.com and CBA for the community center. During the review, the accountants determined that a significant number of transactions had been omitted from the accounting records; other transactions that were included appeared to be grossly inappropriate. This included bank withdrawals that were omitted from the financial records, operating expenses from other venues managed by some of ABC's and CBA's owners, ATM withdrawals and retail purchases without a business purpose, and numerous overdraft fees, just to name a few. The accountants hired by Hillside Acres noted that many of these purchases appeared to be Christmas gifts for families of the CBA partners. There also were numerous purchases of cigars and alcohol, as well as payments to an attorney and traffic safety school.

CBA estimated revenue of US$500,000 during a five-month time period. However, only US$130,000 was included in the financial statements. ABC and CBA did not maintain any calendars or records that would indicate what events were held at the community center or the number of participants. As a result, it was impossible to corroborate the estimates.

ABC/CBA management was also unfamiliar with the basics of employment law, particularly with regard to the classification of employees and independent contractors. They had failed to withhold or remit payroll taxes from any of their employees working at the community center during the previous 17 months. The accountants estimated the outstanding payroll tax liability on wages paid by ABC/CBA to be at least US$50,000 before penalties and interest.

CBA management identified at least US$235,000 in overdue bills payable to various vendors including their utility provider; the accountant hired by Hillside Acres determined that the actual amount due was at least US$311,000. The city worked with CBA and its utility provider to agree on a payment schedule, but CBA never made the first payment due.

The city hired a consultant with extensive parks and recreation experience to conduct an operational review of the community center. He determined that the ice at the rink was overdue for replacement and that Hillside Acres was risking significant damage to the floor and piping at the rink. He also indicated that the building needed to be thoroughly cleaned, and he determined that the insurance purchased by

TO COMMENT on this article, EMAIL the author at jenell.west@theiia.org

ABC and CBA did not meet the requirements specified in the contract. He presented his findings at a city council meeting as the accountants were concluding their review. Shortly thereafter, Hillside Acres canceled its contract with CBA.

Lessons Learned

- Organizations should have procedures in place to monitor vendor contracts. A specific employee should be designated the contract administrator, should be provided with a copy of the contract, and should be responsible for acting as a liaison between the contracting parties. Noncompliance with contract terms should be immediately brought to the attention of both contracting parties for corrective action.
- Because of poor accounting practices, no one at ABC, CBA, or Hillside Acres was able to determine how much revenue was earned and the amount of cash collected by the community center. These missing records permitted CBA and ABC to obscure the profitability of the center, thereby denying Hillside Acres its due portion of the net profits. It is important that both contracting parties work together to design and understand the internal controls in place, particularly over the cash receipts and revenue cycles.
- ABC and CBA maintained complete control over the financial records of the community center. As a result, they were able to easily disguise inappropriate expenditures that were paid using community center funds. Fraudulent payments would have been rapidly detected if a contract administrator or other appropriate professional was responsible for reviewing original financial records, such as bank statements.
- Vendor contracts need to include an audit clause that clearly states who is responsible for paying the cost of the outside auditor and if this responsibility can change depending on the results of the audit (i.e., if there are audit findings, make the vendor pay for the cost of the audit). Sadly, the city was responsible for the external audit fees.

JENELL WEST, CIA, CPA, CFE, *is director of forensic accounting at Rehmann Corp. Investigative Services in Troy, Mich.*

mkinsight
The world's fastest growing
Audit Management Software
+1 847 418 3898 | www.mkinsight.com
Trusted by Companies, Goverments and Individuals Worldwide!

A WORLD CONN

By Jane Seago

The Internet of Things requires internal auditors to confront risks that are not so neatly contained.

Depending on the source you consult, by 2020 the number of internet-connected devices worldwide could range from 26 billion (Gartner) to 50 billion (Cisco). At either end of the spectrum, the number is staggering. Clearly, marketplace forces such as increasingly available broadband internet, decreased cost of connecting, expanded use of the cloud, growing numbers of devices built with Wi-Fi capability and sensors, and the lowered cost of technology have combined to create the perfect environment for the Internet of Things (IoT).

The impact of IoT is already well underway. This latest and perhaps most ubiquitous technology trend, which Jim Tully, chief of research for IoT at

Gartner, London, defines as "a network of physical objects that contain technology that allows those objects to sense and interact with their surroundings and interact with those surroundings for business benefit," is an integral part of our lives (see "Examples of IoT" on page 33). Its fans extol IoT's convenience, speed, personalization, and ease of use. Businesses tout its cost savings, safety enablement, revenue generation, and data-gathering abilities.

However, some view the implications of IoT's billions of connections and terabytes of data and know that the benefits, while substantial, have a dark side: security risks, loss of privacy, and a diminished capacity for people to control their own lives. Kenneth Mory, principal for Stronghold Solutions International and former city auditor for Austin, Texas, states, "The horizon risks that IoT introduces are orders of magnitude beyond those of the present. These new vulnerabilities have grave implications for IT security and cybersecurity."

Internal auditors have distinct reasons to ponder what IoT means for their organization. They may be called on to offer advice to management on the benefits and potential competitive edge IoT can provide. However, they must also monitor the new risks it introduces and the compensating controls required. They cannot afford to assume that something once fixed stays fixed. Just as a high tide raises all boats, the rapid development cycle for IoT means an equally rapid

PHOTO ILLUSTRATIONS: ELESY / SHUTTERSTOCK.COM; MADPIXBLUE / SHUTTERSTOCK.COM; PHOTO MANIPULATION BY SEAN YATES / YACINSKI DESIGN

TO COMMENT on this article, EMAIL the author at jane.seago@theiia.org

evolution of risks. Internal auditors need to stay attuned to these changes and be prepared to keep their organizations apprised.

AN ARRAY OF RISKS

Few would likely disagree that IoT's hyperconnectedness presents risks. There are, however, differences of opinion on the nature of those risks.

Some see the risks in fairly apocalyptic terms. They believe that when everyday activities are monitored and people output information on a near-continual basis, the level of profiling and targeting will grow, leading to increased social, economic, and political struggles. They suggest a need for ways people can disengage from the network, to stop sending and receiving data. Tully considers the disconnect options with some skepticism: "IoT is everywhere," he says. "There's no way to get away from a lot of it."

However, other views of IoT-related risks are more pragmatic: financial loss affecting profitability (a hacker taps into a smart electric meter and steals energy), business interruption (due to a denial-of-service attack), loss of competitive advantage (attacks of any kind by a business rival), governmental upheaval (propaganda or hacktivism), and even loss of life (damage to pacemakers or equipment in hospital operating theaters). Mory points to another risk, loss of market share, which results when "the organization fails to adopt IoT and take advantage of the opportunities and benefits it can provide."

Mory refers to the upside risk of IoT, a perspective that is sometimes overlooked in the very real concern about security and privacy. But there is a reason the IoT market is expanding rapidly, despite the inherent risk: It provides benefits that many individuals and businesses believe outweigh the associated risk. Customers appreciate the way IoT devices make their lives easier by anticipating and addressing their needs and preferences (e.g., constantly adjusting household temperature based on home conditions and homeowners' schedules; brewing a cup of coffee to the individual's precise taste, with the ability to monitor brew status remotely). Businesses that use IoT devices in their own processes, or whose employees use IoT devices, may realize competitive advantage over less tech-savvy rivals, save money through device-generated efficiencies and real-time monitoring, enjoy more immediate and personalized engagement with customers, and reap increased return on their marketing investment through more effective and precisely targeted marketing messages. Companies that manufacture IoT devices are likely to see increased earnings due to customer demand and may even find opportunities to create new lines of business. And everyone, individuals and businesses alike, will benefit from the increased focus on cybersecurity—and resulting adoption of commonly accepted standards and business efforts to earn consumer trust—that IoT devices generate.

"[Internal audit] is a critical ingredient in ensuring the strategy is implemented in a good way, from a risk management perspective."

M.J. Vaidya

Whether the risk is upside or downside, it is a pragmatic issue that presents internal audit an active playing field in which to identify, assess, and mitigate risk. But internal audit cannot serve as the lone outpost on risk. Other areas must engage as well. However, Steven Babb, director and independent consultant at Newton Leys Consulting Ltd., Berkshire, U.K., says that management may not be fully aware of the risk—possibly because it is not articulated in business terms—and that policy has not caught up to define IoT usage. "IoT is typically wrapped up as part of cybersecurity, which is getting increased management exposure, but more still can be done," he says. "Also, IoT covers areas that are typically not

72% of senior IT professionals say that security not adequately designed into products is the biggest challenge facing IoT security, according to the 2016 IOActive Internet of Things Security Survey.

under the remit today of information security departments."

Corbin Del Carlo, director, internal audit, IT security and infrastructure at Discover in Riverwoods, Ill., points to another group that needs to engage in management of IoT risks: software developers (programmers). "A lot of programmers have always dealt with closed systems," he says. "They may not be aware of what connectedness implies. As the third line of defense, auditors need to talk to them and make them aware of the risk."

"The horizon risks that IoT introduces are orders of magnitude beyond those of the present."

Kenneth Mory

BRINGING RISKS TO LIGHT

For Babb, internal audit's role in IoT is "all about visibility and risk—helping risk management teams highlight that the risk is real, quantify the exposure, and bring it to management's attention," he says.

Del Carlo echoes that focus. "We have to challenge threat vectors," he explains. "We have to be willing to offer suggestions of things that could be done to improve security. We have to be willing to ask questions about vendor-driven threats." Del Carlo adds that vendors likely are not manufacturing the devices they produce alone. He questions whether vendors know who is making the parts they rely on in their supply chain. "Are they testing those parts to ensure they are up to our security specifications?" he asks.

Peter Rhys Jenkins, Worldwide Watson IoT architect, IBM, in Dartmouth, Mass., reinforces the need for security throughout the manufacturing process. "I want my refrigerator to be every bit as secure as a government device," he says.

Organizations that implement IoT devices should have a strategy for their deployment. M. J. Vaidya, principal, EY, Atlanta, notes that although the internal audit function may not participate in defining that strategy, "It is a critical ingredient in ensuring the strategy is implemented in a good way, from a risk management perspective."

A productive first step for internal auditors to address IoT is to conduct a risk assessment of the IoT in use in their organization. The risks will vary from one company to the next, depending on the type of IoT systems present and the business process they support. Once the risks are identified, internal audit can ensure that mitigating controls are in place and operating effectively, always keeping in mind the context in which the IoT systems function.

When examining context, it's important to remember that nothing exists in a vacuum. Del Carlo recalls an incident from the 2015 Black Hat USA Conference, during which hackers assumed the challenge of remotely taking over the controls of an internet-connected vehicle. Their approach was relatively simple. The vehicle manufacturer had not implemented password protection on the internet-facing aspect of the car's radio. "The designers felt there was nothing sensitive in the radio, so there was no need to protect it," Del Carlo explains. "And they were right about the radio alone. But that point of entry was the gateway to the rest of the car." Context is everything.

AREAS OF ENGAGEMENT

Taking on the risks associated with IoT is a massive challenge that depends on teamwork across the organization. However, in the spirit of even the longest journey beginning with a single step, there are several initial activities in which internal audit can engage.

Look for a Policy When addressing security-related issues within an enterprise, one of the first steps is to

MORE READ "The Opportunity of Things" on InternalAuditor.org to learn how internal audit can help organizations identify the competitive advantages of embracing the Internet of Things.

determine whether a policy exists and is up to date. While few organizations appear to have an IoT-specific policy at this point, many reference the topic through their "bring your own device" (BYOD) policy. Babb explains that most BYOD policies cover only a small subset of devices that fall under the IoT banner. He adds, "Many of the devices will be brought in by staff, but equally many will be purchased by the organization and used. Of these, many will fall outside the remit of IT and security, so the risks emanating from them may be hidden."

Mory adds that although his previous employer, the City of Austin, had no umbrella policy to deal with IoT, there were policies to address the use of flash, portable drives, and other portable devices such as phones and laptops.

IoT security shortcomings present an opportunity for internal audit to play a significant role by working with the cybersecurity team, IT, legal, and the privacy function to advise on the development of an IoT policy. Existing policies relating to passwords, patching, and system monitoring will need to be revised to place IoT clearly within their scope. New or updated policies may be required around network segmentation and access control. Approved devices and uses must be spelled out, and the implications clearly identified not only for employees, but also for business partners, suppliers, and customers who have connections to the company's network.

Check Inventory Enforcing an IoT policy is difficult without a clear understanding of the number and types of IoT devices present within the organization. Babb and Mory agree that inventories, if they exist, are likely to be incomplete or siloed, as opposed to presenting a comprehensive view. Some inventories may cover devices the organization has purchased, but fail to mention the consumer devices brought in by employees.

Once the inventory provides the needed information, appropriate controls can be put into place. Del Carlo's company, Discover, places a priority on protecting its network. "We have a general ban against non-company devices," he says. "We won't allow them onto our network. We provide a 'guest' network people can use to connect those devices; all they can get is the internet." Discover also installs virtualization software on the phones it provides to segment the data, and it has a stringent perimeter defense system. Laptops are encrypted and the data can be wiped remotely. Even then, Del Carlo notes, "Every day these controls block hundreds of exploits from attackers of various sophistication levels. But without constant vigilance against the onslaught, it is unlikely any organization could stop every single attack."

Educate Management Regardless of management's degree of awareness about IoT risks at this moment, there seems to be consensus that some additional education would be useful. Mory says that some management is aware of the general concepts behind IoT, but lacks a core understanding of the opportunities and threats it presents. In his view, internal audit has a clear role to play in helping management understand and manage the risks.

Vaidya agrees that education is important, "from the board level to the tactical level and across not just IT, not just executives, not just product development, not just manufacturing, but across the business."

Review Security Jenkins lists some basic but necessary steps auditors can test after implementation. "With regard to provisioning, when a new device

"IoT is typically wrapped up as part of cybersecurity, which is getting increased management exposure, but more still can be done."

Steven Babb

EXAMPLES OF IoT

Many IoT devices are so well embedded in everyday, modern life that we may not realize they are there. But IoT abounds, as indicated by this small sample suggested by Jim Tully, chief of research for IoT at Gartner, London:

- Cars: Modules track a driver's behavior—how he or she accelerates, takes the corners, stamps on the brakes. This information allows insurance companies to match the risk of individual drivers with their own specific premium. It can also enable insurance companies to offer "pay as you go" insurance, in which the premium is determined by the amount of time the car is driven or where it is—on a remote country road or in a big city at rush hour.
- Parking: Sensors monitor city streets and determine whether parking spots are being used. They then link to a mobile app that guides the driver to an available spot.
- Lighting: New lighting can track the location of people in buildings, providing safety benefits (ensuring their area is lighted) and cost savings (shutting off lights in unoccupied spaces).
- Toys: Some toys are equipped with cameras that can recognize the faces of individual children. They can then "learn" about those children and interact with them in a highly personalized way.
- Agriculture: Sensors in the fields track moisture and sunlight, suggest better use of irrigation, and even predict the timing of the harvest.
- Government: Many cities employ IoT-enabled "smart city" apps to handle tasks such as pollution monitoring and traffic management.

"Without constant vigilence against the onslaught, it is unlikely any organization could stop every single attack."

Corbin Del Carlo

joins the cloud for the first time, make sure the mechanism used to connect is encrypted," Jenkins says. He also advises verifying that the cloud itself is secured, password hashes are stored away from other related identification, and data coming from and to devices is encrypted. Jenkins adds: "Over-the-air firmware updates are necessary to keep equipment up to date. Make sure that process is done securely."

GETTING A HANDLE ON IoT

It seems impossible to discuss IoT for any length of time without landing back at a mention of risks. But Tully points out that quite a few IoT devices are deployed for safety. They exist to reduce risk. "Take structural sensors in bridges, for example," he notes. "These sensors warn of excessive loads and stresses—they are linked to traffic control systems that will stop traffic entering the bridge. Internet-connected carbon monoxide detectors and smoke detectors are similar. They are deployed directly for risk reduction."

But most in the internal audit and information security fields might argue that it's not the purpose of the device that worries them—it's the connectedness and the near-certain impossibility of completely securing an organization, its assets, or the people who use the systems. Del Carlo agrees, but he won't stop trying to lock it down. "There's a saying that you can't make anything foolproof because fools are so ingenious," he says. "But we can't just give up. I work for a bank. We are where the money is—literally. We have to maintain the highest possible level of security."

IoT offers internal auditors an opportunity to serve in a role they don't often get to inhabit: advocate. They can stand up for individual and enterprise users of IoT devices. "Installing security inside IoT devices is difficult and time-consuming, but necessary," Jenkins says. "The companies that manufacture the devices say they are doing it, and doing it well. But, are they? Internal auditors need to make them prove it." Ia

JANE SEAGO *is a business and technical writer in Tulsa, Okla.*

Internal audit should work collaboratively and proactively to address breaches and build resistance to future attacks.

Arthur Piper

Despite banks spending billions of dollars to protect themselves against cyberattacks, financial regulators remain unimpressed. Mary Jo White, chairman of the U.S. Securities and Exchange Commission, told the press in May that cybersecurity was the biggest risk facing the financial system, but banks' "policies and procedures are not tailored to their particular risks." Regulators in Europe also want action. Chairman of the European Banking Authority Andrea Enria—again in May—urged national regulators to stress test European financial institutions to see how vulnerable they were to hackers. If they fail, he said, they should be forced to hold more capital.

And as if that were not enough, SWIFT, the financial payment system that handles more than US$6 trillion in transfers every day, has unveiled a customer security program that includes plans to audit its 11,000 member institutions to check that their security is fit for purpose. "We will look into if and how customers' compliance to these baselines can be made transparent to, and enforced by, counterparties, regulators, and ourselves," SWIFT said. Members will have to share more information and tighten the security of their systems.

The pressure to strengthen IT platforms and applications has come in the continuing wake of high-profile cyber failures. Three of SWIFT's members, for example, have been hacked in the past seven months—including the Bangladesh central bank. Hackers got ahold of the SWIFT codes and transferred US$81 million from its accounts at the U.S. Federal Reserve.

It's not just banks at risk, either. According to recent data released by the U.K. government, two-thirds of big U.K. businesses have been hit by a cyberattack in the past year. Most of the attacks involved viruses, spyware, or malware, the Cyber Security Breaches Survey said in May. It found that one in four large firms said they were breached once a month—sometimes

PHOTO ILLUSTRATIONS: ELESY / SHUTTERSTOCK.COM; ANDRIY SOLOVYOV / SHUTTERSTOCK.COM; PHOTO MANIPULATION BY SEAN YATES / YACINSKI DESIGN

CYBER RESILIENCE

AUGUST 2016

more—and that attacks could cost millions of pounds to rectify. The volume, frequency, and sophistication of attacks are a game changer.

NOT IF, BUT WHEN

Many organizations are now working on the assumption that a cyber breach is inevitable and that they need to have rapid and effective response mechanisms in place to minimize damage. Internal audit departments are being called upon to help—providing everything from improved diagnostics to help locate where, when, and how a breach has occurred, to assistance with the very effectiveness of a business' cyber breach response team.

"People now have to be in a posture that assumes you have been breached, rather than saying that you are never going to be breached," Kelly Barrett, senior vice president of Home Services and former vice president of internal audit and corporate compliance at the Atlanta-based retailer The Home Depot, says. "That mindset changes the way you structure your security program."

Barrett knows through painful experience what a data breach is like. She says no matter how much money a company spends on its defenses, hackers are likely to get ahead of the game through new techniques, or by attacking the most vulnerable part of the business or its supply chain. In addition to beefing up external defenses, Barrett advises organizations to think about what software can be used to pick up behavioral anomalies, such as employees logging into systems at unusual times or unexpected places, within the business, too. While such tools are sophisticated enough to run from day one, they improve over time as the IT team learns how the business works and eradicates any false positives the system may throw at them.

"The key point is that you are now assuming somebody may be looking at things, or using them, inappropriately," she says. "And so the tools you use need to be much more proactive in looking for those unusual patterns."

COLLABORATION

Home Depot's audit team has been working with the chief information security officer (CISO) to think through the design of such programs, understand how the tools work, and ensure that they are actually controlling what the business intends them to control. Internal audit wants to know that the company is getting the full benefit from the technology it has invested in and that those people reviewing the outputs are accountable. That has also brought about a change in how audit operates in this area.

"Internal audit partners very closely with the CISO," Barrett says. "They're not sitting back and waiting to do an audit after the fact. They're actually helping them look at the tools."

Barrett realizes that some may question internal audit's ability to remain independent, but she is clear that as long as internal audit is not implementing controls, that can be achieved. What is powerful about the partnership, she says, is its ability to bring together security experts with auditors who have an equally strong grasp on controls in a way that is proactive. In fact, Barrett is the chair of the company's data security and policy governance committee, which helps her—and the organization—achieve a helicopter view of the security procedures across the business. "That helps us make sure all the different pieces are being considered, and we are thoughtful about what the response is," she says.

"Three to five years ago, IT risk professionals may not have been given as much time on the agenda as they are today."

Gary Pollack

Incident **response teams** reduced the cost of data breach resolution by **US$16** per record, according to IBM and the Ponemon Institute's 2016 Cost of a Data Breach Study: Global Analysis.

"From an audit point of view, the main thing is that we get assurance that ... there is an incident response plan linked with the business' recovery plans."

Nigel Lewis

In the U.S., at least, some of the impetus for smarter working and multidisciplinary cyber defense and reaction programs has come from the board as much as from those working within organizations. If there has not been a revolution that has catapulted cyberrisk to the top of the risk agenda exactly, there has been steady evolution, says Gary Pollack, senior vice president, Assurance Services Leader, American Express Co. in New York.

"Three to five years ago, IT risk professionals may not have been given as much time on the agenda as they are today," he says. "We are clearly seeing an uptake in time allotment in audit and risk committees dedicated to information security and overall IT risk. It's given us a seat at the table."

BEING PREPARED

Pollack says, eventually, regulators are likely to mandate specialist IT skills on boards and risk committees. He says he has seen an increase of IT skills in people occupying these positions and expects that to increase as organizations continue to enhance their risk management practices.

For now, what is important for Pollack, as with many CAEs, is that customer trust in data protection is given top priority in the way that businesses respond to cyberattacks. "We have been aware for quite some time of the need not only to have a preventive strategy, but also a detective strategy," he says. "There is a real need to consider a well-balanced approach to prevention and detection, as well as response mechanisms."

Customer data should be given top priority in a cyberattack response.

Pollack says his organization has a dedicated team and protocols in place to respond to breach incidents ranging from how to communicate, escalate, and react timely to threats and attacks. From an internal audit perspective, that means Pollack's team puts equal weight on auditing the preventive and detective parts of breach management controls, protocols, and escalation mechanisms. Audit also participates as an observer during test scenarios aimed at finding weaknesses in those systems before a breach occurs.

"Audit generally acts as an observer during test scenarios and as a reviewer of the results and action items," he says. Audit then follows up on any actions that have been agreed on to make sure management deals with them. It also flags any gaps in defenses or reaction procedures and makes sure management fixes them.

BREACH RESPONSE

Auditors agree that having an appropriate response plan in place for a breach is critical—one that has been tested and retested before the event arises. While it would be rare for internal audit to take charge of such a team, it has a critical role to play, says Nigel Lewis, an independent audit consultant and trainer.

"From an audit point of view, the main thing is that we get assurance that someone will take charge of the incident response team and that there is an incident response plan linked with the business' recovery plans," he says. The size of the team depends on the nature of the organization, he says, but even large businesses would typically appoint only 10-15 people to it, split roughly two to one between IT

experts and business executives. In an incident, those team members would call on their own teams to implement any remedial action needed.

"Part of the incident response will be pages and pages of plans detailing who does what and what the key activities are," he says. "Auditing that process is important." But what should it comprise? Lewis says auditors can cut through the complexity by dividing the process into three parts: reaction time, decision-making, and action.

Although more than eight in 10 breaches are detected within 24 hours, according to the latest U.K. government statistics, it can take months to detect a breach. In 2013, for example, *The Wall Street Journal* said Chinese hackers had infiltrated its systems for four months without detection. That does not mean swift action isn't important once a hack is detected. The business needs to do a quick impact analysis to see what type of breach the team is dealing with. Fraud, breaches of confidential data, denial of service, intellectual property, and ransoms — the business needs a plan for each with specified response times. A denial of service attack, for example, is likely to need a faster technical reply than, say, a ransom demand. "You must know how quickly you can respond to each area and be able to test it," Lewis says.

Many of the decisions a business might need to make can be preplanned, too. And it is vital to know what the impact of those decisions are likely to be on the organization's operations, staff, customers, regulators, and the media. Then it is time to put those decisions into action. Deciding which systems to close down and for how long is never easy, but being prepared makes it less likely the breach will turn into an all-out disaster.

"For all of this to work well, you need a good team, convened quickly, and comprising the right experts," he says. Bringing in external support can be important, and keeping people up-to-date with the latest attack methods and breaches is essential.

If that sounds straightforward, it might be puzzling to know that 37 percent of firms have no cyber response plan, according to PricewaterhouseCoopers' (PwC's) 2016 Global Economic Crime Survey. That is because while businesses feel they have response systems in place, they tend to be structured to deal with classic threats such as flooding or power outages, says James Rashleigh, a cybersecurity director at PwC. "While they think they're prepared, they suddenly find out when they suffer a cyber breach that they're dealing with something very different." Businesses that have not nominated a specific leader for the response team, or have someone from the IT team in charge, are not likely to be able to cope well as the issues are too wide-ranging. For example, breaches affecting customers may be subject to litigation, and putting together what happened from a legal perspective is complex.

CYBER GOVERNANCE

Organizations that do not yet have a sound response team in place could do worse than go back to basics. "Cyberrisk is about protecting the customer," says Liz Sandwith, a former Chartered Institute of Internal Auditors (IIA–U.K. and Ireland) president, and now chief professional practice adviser at the institute. "So we do all sorts of really great audits in the business space, but this goes beyond that into the real world of our customer base."

That makes cyberrisk a business issue rather than a technical IT issue, although she is not convinced that many auditors in the U.K. have actually grasped what this distinction

> "We do all sorts of really great audits in the business space, but this goes beyond that into the real world of our customer base."
>
> Liz Sandwith

Only 25% of respondents with business continuity plans provide clear, specific procedures in response to a data breach or cyberattack, according to The IIA's 2016 Pulse of Internal Audit report.

means. Behind every IT risk is a business risk, and it is the significance of the latter that can be overlooked when focusing solely on technical fixes and controls. In Sandwith's view, auditors should decline to engage solely with IT technicians and insist that people from the business also are involved so the significance of the issue to the business is understood and controlled. While those getting a better grip on the issue might do a thorough risk assessment of the threats their organizations face, she says they also need to consider the board's risk appetite.

Audit needs to understand IT from a technical and controls perspective.

"Internal audit has to make the board and the audit committee aware that it's not just one of those risks where we do our work and make sure it won't happen," she says. "Cyber is a risk that is always going to be a risk."

She says there is an opportunity for risk management and internal audit to work better together by focusing on the business risks from a resilience perspective. That involves members of the audit team really understanding IT risk from a technical and controls perspective and working with risk management to provide intelligent assurance

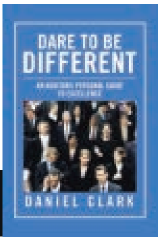
TO COMMENT on this article, EMAIL the author at arthur.piper@theiia.org

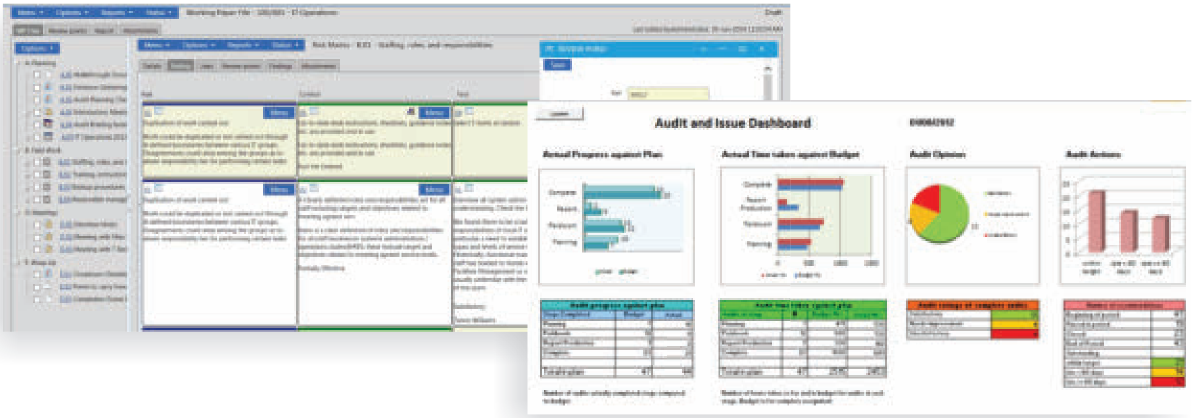
around its controls. She says working across all lines of defense — management, risk, and audit — is critical if a business is to detect and respond effectively to cyberattacks, as no one function has the skills and scope to do it alone. But audit must be a leader in the process. "There is a real risk that without the right skills and knowledge, internal audit could provide false assurance — naïve assurance — to the board and the audit committee," she says.

In addition, Sandwith urges auditors to help establish an effective governance structure around cyberrisk, with defined risk appetite statements pertaining to each threat. Auditors can help ensure the business has information security, risk management, social media, and system access policies that are well-formulated and disseminated across the organization. Finally, she says, the CAE must keep the board engaged with cyberrisk as a living issue.

"Let's not talk technical at board meetings," she says. "This is about the impact on customers, reputation, profits, and share price — as well as potential sanctions for getting it wrong. That's what gets the attention of the board." And it gets the attention of the regulators and the public, alike. As society gets used to the idea that breaches are an inevitable part of online life, competitive advantage will fall to those who respond best.

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




Audit and Issue Dashboard
Actual Progress against Plan
Actual Time taken against Budget
Audit Opinion
Audit Actions

AUDITING THE CLOUD

Jared Rittle,
Jill Czerwinski,
and Michele Sullivan

Internal auditors should delve into the complexities and unique risks of moving to a cloud platform.

All types of organizations are relying on cloud computing to improve performance and reduce costs. Pharmaceutical company Pfizer Inc. uses the cloud's elasticity to increase its computing and analytics power during peak periods of drug development to levels not feasible in a traditional data center. Professional services firm Towers Watson says it is saving 40 percent on costs by using a combination of cloud and company-managed servers to help its insurance clients set auto policy rates based on individual drivers' behavior. Using cloud infrastructure to bypass lengthy technology build cycles enabled Dow Jones and Co. to quickly introduce its financial solutions to the Asian market.

Such successes are a big reason why cloud infrastructure growth is outpacing data center infrastructure growth by more than 46 percent (see "Cloud Computing's Dramatic Growth" on page 45). Commissioning a cloud service provider can enable an organization to off-load much of the difficulty that comes with implementing, maintaining, and physically protecting the systems required for

company operations. The organization no longer needs to employ a large team of network engineers, database administrators, developers, and other technical staff. Instead, it can use smaller, in-house teams to maintain the cloud solution and keep everything running smoothly. Moving to the cloud also can introduce new capabilities, such as the ability to add and remove servers based on seasonal demand, an option that would be impractical for a traditional data center.

With cloud computing becoming mainstream, internal auditors need to devise new ways of pinpointing the risks these services pose and verifying the security, reliability, and availability of critical data housed by an outside provider. Based on this assessment, internal auditors can advise their organizations about choosing a cloud service provider and preparing for the challenges of overseeing the cloud platform and infrastructure.

THE CHOICES AND COMPLEXITIES AHEAD

The cloud encompasses application service providers, cloud infrastructure, and the virtual placement of a server, set of servers, or other set of computing power in an environment that is shared among many people and organizations. Cloud platforms and servers extend and supplement an organization's own servers, resulting in multiple options for computing and application hosting.

It is not sufficient to think of cloud platform and infrastructure oversight as mere vendor management. Internal auditing of these environments is more complex, because of several factors about which the audit function needs to make decisions when determining the audit scope.

No Two Clouds Are the Same A cloud deployment can be just as variable as a traditional IT implementation. Among the numerous cloud platforms, the most common are infrastructure as a service, software as a service, and platform as a service. Using these three options alone makes a wide variety of models and other options available. Each of these options poses a different set of risks and controls, depending on an organization's specific deployment of a particular cloud platform and infrastructure.

In some cases, auditing the cloud provider's processes and infrastructure might not be allowed.

Third-party Barriers Many challenges and barriers to the audit appear when an organization is dealing with a third-party vendor. In some cases, auditing the cloud service provider's processes and infrastructure might not be allowed. In its place, the vendor may offer attestation reports such as the American Institute of Certified Public Accountants' (AICPA's) Statement on Standards for Attestation Engagements No. 16 (SSAE 16) as evidence of organizational controls. In other cases, the provider might restrict the audit to a select portion of the service. Further, providers often require the client to obtain specific approvals before any audit activities can begin. An organization should take these types of considerations into account before contracting with a cloud vendor.

PHOTO ILLUSTRATIONS: ELESY / SHUTTERSTOCK.COM; TAIRA / SHUTTERSTOCK.COM; PHOTO MANIPULATION BY SEAN YATES / YACINSKI DESIGN

Top cloud security concerns are: difficulty migrating services or data (27%), high costs (25%), and lack of visibility into provider operations (25%), according to Intel Security's Blue Skies Ahead report.

CLOUD COMPUTING'S DRAMATIC GROWTH

In the most recent edition of its annual IT Spending & Staffing Benchmarks report, market research firm Computer Economics describes 2015-2016 as "a tipping point where investment in cloud applications and infrastructure is rising." According to the annual survey of more than 200 IT organizations across 23 industry sectors in North America, "a net 56 percent of IT organizations currently are increasing spending on cloud applications compared with a scant 10 percent that are growing spending on data center infrastructure."

Other analysts make similar projections. *Forbes'* "Roundup of Cloud Computing Forecasts and Market Estimates, 2016" found double-digit growth for various cloud computing specialties and services across more than a dozen industry surveys, with cloud industry revenues of more than US$100 billion.

Control Responsibilities Are Shared One of the most difficult aspects of auditing a cloud infrastructure deployment is determining which controls are to be managed by the organization and which by the cloud provider. With many cloud deployments, few controls are actually the responsibility of the provider. For example, the organization itself may be responsible for configuration management, patch management, and access management, while the provider is only responsible for physical and environmental security.

> Migrating to cloud-based services can dramatically alter the risk profile of any organization.

Tracking Cloud Deployments Is Difficult An organization's physical assets are tangible. The organization buys a physical piece of equipment and keeps a record of this asset; an auditor can see all the organization's technology assets by walking through the data center. Cloud infrastructure deployments, however, are virtual, and it is easy to add and remove these systems. Many organizations base their models on servers and systems that are there one day and gone the next. IT departments also struggle with managing cloud assets, and tools to help cloud providers are evolving. As a result, the audit scope is hard to manage.

Cloud Infrastructure Expertise Is in Short Supply Because cloud computing is a relatively recent and fast-growing technology service, an organization's employees may not have cloud expertise. This scarcity creates risks because IT administrators aren't positioned to explain the details of the cloud deployment, and internal auditors aren't trained to interpret and assess deployments.

CLOUD RISK ASSESSMENTS

Migrating from facilities that are operating internally to cloud-based services can dramatically alter the risk profile of any organization. For example, when an organization moves to a cloud-based service, in most cases, all of its data is stored on the same physical equipment where other organizations' data is housed. If configured inappropriately, data leaks could result. Following leading audit practices, internal auditors first must perform a cloud risk assessment to identify the specific risks and controls associated with their organization's deployment strategy. A thorough

TO COMMENT on this article, EMAIL the author at jared.rittle@theiia.org

assessment is needed, regardless of whether the organization is contemplating hiring a cloud service provider for the first time or is considering expanding its business with a provider. Internal auditors should incorporate several factors into the risk assessment of their organization's cloud platform and infrastructure.

Strategy Interacting with the organization's IT and business leadership is the auditor's first step toward understanding the organization's cloud strategy. How does the organization expect to use the cloud, and what are the benefits of using it that way? What is the scope, from a macro perspective, of the organization's plans for cloud deployments? The lack of a cohesive, formal, and well-aligned cloud infrastructure strategy should be a red flag for an internal auditor.

Personnel Part of the organization's cloud strategy should be a staffing strategy for the three lines of defense functions. Cloud servers don't run themselves. While fewer employees might be needed because of the absence of physical equipment and the ease of maintenance, experts in all three lines need to be trained and available to address the risk, according to their role. Organizations should consider training options available from the Cloud Security Alliance, CompTIA Cloud Essentials, and Rackspace Cloud University. Moreover, CAEs should consider how they will staff the audit and whether assessment of personnel qualifications to

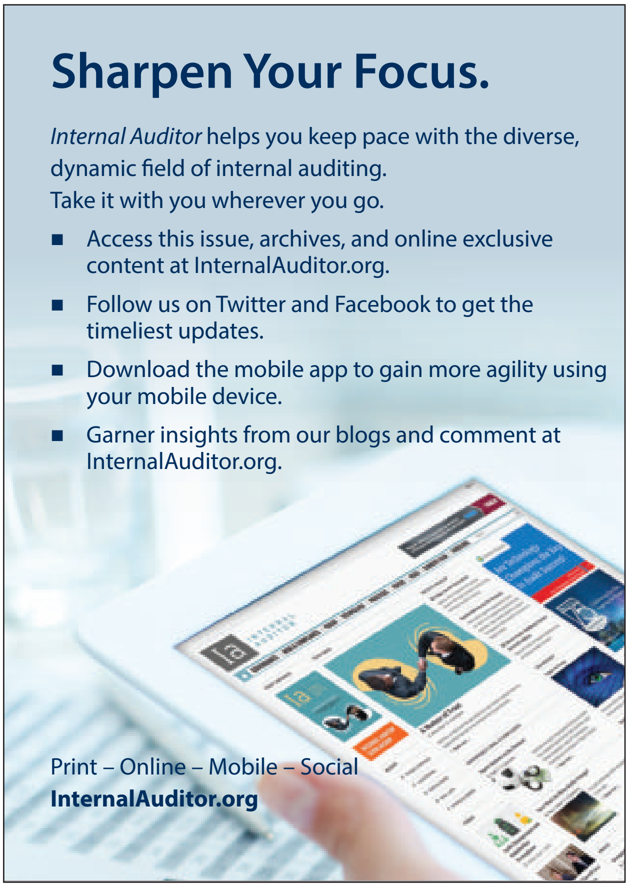
40% of respondents say their organization processes or stores sensitive data such as business intelligence and financials in the cloud, SANS Orchestrating Security in the Cloud survey reports.

manage the cloud deployment should be in scope for the risk assessment.

Security Program IT departments and business units should have a cloud security strategy. A strategy includes determining the type of data permissible to store in the cloud and how its security will be enforced. It also includes the integration of the information security program into the cloud. All the usual IT risks of traditional data centers apply to cloud deployment as well—among them, malware propagation, denial of service attacks, data breaches, and identity theft—all of which, depending on the implementation, can fall to either party.

Professionals who have received training in cloud computing may be able to adapt traditional IT programs for auditing servers in physical form to a cloud environment. There's more good news: Cloud infrastructure brings with it myriad security technologies that are not affordable in traditional deployments such as identity and access

> **Cloud infrastructure brings with it security technologies that are not affordable in traditional deployments.**



management systems, network segmentation, and multifactor authentication.

Penetration Testing All systems, including systems in the cloud, have the potential to be hacked. Many cloud service providers test their environment regularly to analyze their ability to withstand wide-scale attacks. This testing, however, rarely covers the deployment specific to the cloud customer. Organizations should contract separately to have a penetration assessment of their cloud infrastructure conducted periodically. Doing so requires written authorization from the vendor, which is likely to be provided, as long as the requesting organization follows the rules specific to the cloud service provider's individual system. Obtaining the provider's authorization can be time-consuming, so cloud clients should plan far ahead.

Reliability and Redundancy Internal auditors must understand the organization's expectations for resilience from disruption. Because IT departments often have too few people or an insufficient budget to implement reliable and redundant systems in a self-managed infrastructure, many look to the cloud for a solution. Management might assume that redundancy is automatically built into the service provider's infrastructure, but frequently that assumption is incorrect. Rather, organizations need to intentionally deploy redundant environments in the cloud.

NOT JUST ANOTHER VENDOR ASSESSMENT

Overall, internal auditors should not approach a cloud engagement in the same way they approach other third-party vendor audits. Cloud engagements present their own complexities, which auditors must understand to assess them adequately. SSAE 16 and other attestation reports based on audit and attestation standards are valuable, but they are not sufficient.

A correctly implemented cloud infrastructure can actually reduce an organization's residual risk by offloading a portion of the responsibility for managing IT risks to a cloud service provider. Internal auditors have a valuable opportunity to see that their organization is benefiting from the cloud while adequately addressing the new risks that are introduced when their organization contracts with a service provider and moves IT operations to the cloud. Applying the same level of rigor to cloud technology that they previously applied to technology managed in-house creates an environment in which the internal audit function can be a primary advocate for a strong cloud strategy that is implemented within the organization's risk tolerance.

> **SSAE 16 and other reports based on audit and attestation standards are valuable, but they are not sufficient.**

JARED RITTLE *is a technology risk consultant with Crowe Horwath LLP in New York.*

JILL CZERWINSKI, CISSP, CISA, CIPP, *is a technology risk senior manager with Crowe Horwath LLP in Chicago.*

MICHELE SULLIVAN, CPA, CRMA, *is a partner with Crowe Horwath LLP in South Bend, Ind.*

Control self-assessments can increase audit efficiency and spread control awareness throughout the organization.

Trust but Verify

Parikshith Acharya

“Trust but verify” is an old adage that is apt for the internal audit profession. It is the core principle of control self-assessment (CSA), which requires internal auditors to place a relatively high degree of reliance on trust in the process owners’ judgment, while also verifying the accuracy of their assessment.

CSA is an assurance and audit approach that enables process owners to self-evaluate the effectiveness of their controls to mitigate risks. Management and internal audit can use CSAs collaboratively to assess the adequacy of their organization’s risk management and control processes

PHOTOGRAPH: CHANPIPAT / SHUTTERSTOCK.COM

through techniques such as facilitated team workshops and questionnaires.

The internal audit department at Hewlett Packard Enterprise (HPE) has implemented a CSA framework to help it provide assurance on key risks across more than 150 countries and businesses, ranging from hardware and software to services. Auditors use CSAs to perform audit engagements in business units where it is not feasible to deploy a full-fledged audit team. This approach has enabled the department to provide quicker, relevant, and focused assurance while also promoting awareness of controls among business process owners.

DEVELOPING A FRAMEWORK

HPE's internal audit function performs various types of audits such as individual country and legal entity audits, regional and worldwide horizontal business-process audits, and individual contract audits. The department's first task was to decide which type of audits should be included in the CSA pilot. The department chose to use CSA for country audits because they typically include review of certain standard scope areas such as procurement, employee expense claims, and statutory compliance. Moreover, it decided to try out CSAs in countries with a relatively small volume of operations but with inherent risks such as high perceived corruption. It also selected smaller countries, where the business used local processes and IT systems, rather than the company's standard corporate tools.

The real test in developing the CSA framework was explaining the approach to management and process owners.

The next step was to create a list of standard risks for the processes typically reviewed in such audits and map the existing controls, leveraging internal audit's knowledge and audit programs from past engagements. Auditors developed a simple, spreadsheet-based tool to document this risk and control list and to provide the potential respondents an easy method to assess and rate their respective controls as being effective or ineffective. The tool also provides a section to enable respondents to provide additional comments in support of their assessment. These two steps took four months to complete, because the department needed to decide how to pilot its CSA approach, review numerous iterations of it, and update the tool to ensure that the risk and control coverage was comprehensive and accurate.

THE PILOT ASSESSMENT

The real test in developing the CSA framework came when auditors had to explain this approach to management and process owners to get their support for participation. It was important to identify the relevant stakeholders from management who could support and participate in the CSA pilot. After careful consideration, the department selected the country finance controllers who could act as coordinators to help drive responses from the various process owners and provide a consolidated self-assessment for the entity under review.

Although business process owners raised many questions and concerns during this phase, one of their most common questions was, "Does performing a self-assessment mean we won't be subjected to internal audits again?" The department spent considerable time explaining that while self-assessments would rely to a high degree on self-evaluation, there would

Internal control is "the responsibility of everyone in an organization and therefore should be ... part of everyone's job description," according to COSO's *Internal Control–Integrated Framework.*

still be some independent review and validation from internal audit to assess the accuracy of those assessments. These would be relatively lighter audits, and the CSA exercise would benefit the business by increasing self-awareness of controls.

During the pilot self-assessment, the respondents reviewed the risk and control statements and rated their respective controls as being effective or ineffective. Throughout this four-week phase, internal audit held frequent checkpoint meetings with the respondents to clarify queries from the process owners, typically to interpret certain control statements in order to assess their effectiveness.

Once the process owners had completed the self-assessments in the tool and submitted them, internal audit needed to decide on the best approach for the independent validation of the results. While most of the controls being rated as effective provided a degree of comfort, auditors still had to objectively review the accuracy of the assessments while also balancing the level of review to avoid converting it into a full-blown audit.

Internal audit reviewed the self-assessment results and comments in detail, and performed additional procedures such as walkthroughs, process interviews, limited sample testing, and analytics to verify the assessments. The department particularly focused on certain effective-rated controls that auditors had assessed as key controls or mapped to critical risks. For example, auditors conducted more detailed testing of controls that had audit issues noted from past audits to verify that the current effective self-assessment was justified. Internal auditors treated controls rated as ineffective as self-reported issues, and the team assessed whether an appropriate root cause analysis of the issues had been performed and made recommendations where management action plans were pending.

Internal audit reported the final results using the audit report format with which the process owners and senior management were familiar. Engagement ratings reflected the extent that self-assessments were accurate.

CSA BEST PRACTICES

Internal audit departments can adopt some best practices to help overcome the challenges that may impede the effectiveness of CSAs:

- » **Get the right level of project sponsorship.** Explain the CSA approach and benefits to key senior management personnel at the initial stage, and visibly involve them while rolling out the CSA project to ensure the right level of response and involvement by process owners.
- » **Provide training.** Conduct training sessions at the kick-off stage to introduce internal audit's concepts of risks and controls to potential CSA participants.
- » **Speak the language of the business.** Create a self-assessment tool containing a listing of standard risks and controls, using the same terminology that the business process owners use, which will make it easier for them to comprehend.
- » **Provide continuous support.** Conduct periodic status update meetings with the CSA participants to clear their doubts or queries in the process, thus making it a guided self-assessment.
- » **Perform an independent review.** The audit team should follow up the self-assessment phase with an independent validation of the results. This can involve enhanced walkthroughs, analytics, and limited sample testing to assess the accuracy of the self-assessment, especially for controls that have been rated as effective.

EARLY LESSONS

The pilot and subsequent engagements yielded lessons for the internal audit team and business units. One interesting lesson arose in cases where the process owners rated a control as ineffective, but internal audit's subsequent independent testing revealed that the issue at hand was either a one-off exception or immaterial and was not necessarily a control design or effectiveness gap. This emphasized the importance of training the respondents in risk and control concepts at the project kick-off stage, as well as throughout the engagement, to avoid false positive or false negative results.

Buoyed by the success of the CSA for the country audits, internal audit rolled out this approach for a business unit-focused audit of HPE's services business. For this audit, the audit function explored a different approach by partnering with one of the service business' compliance organizations—another assurance provider—to obtain buy-in from participants and conduct the pilot assessment. Although adding another layer increased the time needed to roll out the CSA, it proved more effective because internal audit could leverage the business knowledge and relationships that the compliance organization already had. This made the CSA tool more relevant, accurate, and acceptable. Realizing the benefits from the pilot, the services business is now considering using the CSA tool as a mandatory document to be updated and maintained by its various teams along with conducting a periodic self-certification exercise.

CSA enables internal audit to allocate resources to focus on areas with significant control weaknesses.

Another variant of the spreadsheet tool was to create a CSA survey containing control statement questionnaires using a Microsoft SharePoint-based form. This was particularly useful where the number of respondents was great and spread across multiple locations and time zones. This approach also was ideal for assessing the risks and controls for a single horizontal process at a worldwide or regional level or for prescoping and risk assessments.

Despite these early successes, HPE's internal auditors faced several challenges in implementing the CSA framework. The problems included educating respondents on risk and control concepts, drafting the control statements in an easy-to-understand manner, and ensuring timely completion and submission of the self-evaluations. The internal audit function resolved each of these problems through patience, constant and open communication, and by being flexible to adapt the tool and process based on inputs from the business-process owners.

Finally, one of the important tasks for internal audit was to codify and standardize the lessons it learned to ensure that the approach is consistently implemented by auditors across HPE's global locations. Internal audit accomplished this by developing a guidelines document that provides best practices and a suggested methodology for independent assessments.

CREATING CONTROL AWARENESS

The success of the pilot assessment spurred many more CSA audit engagements at HPE, and CSAs have become an accepted approach and an integral part of internal audit plans. Based on internal audit's experience, CSA reinforces management's responsibility for risk management and aids increased control awareness among business-process owners. From an internal audit viewpoint, it facilitates optimum use of resources, enabling the department to allocate resources to focus on areas with significant control weaknesses. The CSA can be used as a continuous control monitoring tool that facilitates "light touch"-focused audits. Above all, managers value internal audit's CSA approach and tool for enabling them to carry out their risk management responsibilities.

As with everything else, CSAs come with their own challenges (see "CSA

TO COMMENT on this article,
EMAIL the author at parikshith.acharya@theiia.org

Best Practices" on page 51). They can be difficult to execute in organizations with rapid corporate change, high turnover, and decentralization. Some business-process owners may not have adequate understanding or share internal audit's understanding of risk and control concepts, which may result in inaccurate assessments. Also, there is always the inherent risk that process owners may be naturally inclined to assess their controls as being effective, hence the need for internal audit to exercise the right amount of professional skepticism during its independent review.

A CSA framework can enable higher audit efficiency and increased control ownership among management. In addition, CSAs can provide a knowledge repository of controls and educate new audit and business-unit employees about those that are relevant. Organizations should tailor their CSA approach to meet their specific business and audit requirements. Moreover, they should review and update their framework constantly to keep it in line with changing business models and the resulting risk and control environment.

> **CSA can provide a knowledge repository of controls and educate new employees about those that are relevant.**

PARIKSHITH ACHARYA, CIA, CA, CISA, *is manager-Internal Audit at Hewlett Packard Enterprise in Bangalore, India.*

AUDIT

NEVER SLEEPS

IIA Global Chairman of the Board ANGELA WITZANY says internal audit's ability to remain relevant hinges on ceaseless attention to the priorities of the organization it serves.

We live in an "always on," 24/7 society. Our devices keep us continually connected, businesses are available around the clock, and fast turnaround cycles are the norm. We expect uninterrupted access to information and rapid delivery of products and services. Our world is hyperconnected and in constant motion.

As part of this new reality, risk and change have become corporate constants. New risks are always emerging, requiring internal audit to continually scan the horizon and keep pace with the latest developments. We need to be constantly aware of what's happening in the organizational environment, the regulatory environment, and the profession. And we need to do all of this at the blistering speed of today's business world.

Thus, I have chosen the theme "Audit Never Sleeps" for my IIA chairmanship. In this day and age, internal auditors cannot afford to rest on their laurels. We must provide innovative and proactive pathways for improvement and continuously offer solutions. We should take every opportunity to strengthen our brand, build trust, and cultivate relationships. We need to be ever-vigilant in our approach to risk and never diminish our focus. Internal audit's ability to remain relevant hinges on ceaseless attention to the priorities of the organizations we serve.

My theme connects as well to the founding place of The IIA—New York, "the city that never sleeps." Since The Institute's inception in midtown Manhattan 75

Photographs by Ian Ehm

years ago, internal auditors have worked tirelessly and passionately to meet the evolving expectations of stakeholders. We need to continue that momentum, and build on it, as we work toward serving our clients in the current age of constant activity and perpetual movement. By honing our communication skills, adopting an integrated mindset, doing the right thing, focusing on strategy, and keeping an eye toward the future, we can help pave the way toward an even more proactive, business-centric focus.

COMMUNICATE WELL

Effective communication is crucial to our work with stakeholders. Management and the audit committee expect us to provide insights into the business, and those insights need to be delivered in a way that is not only heard but also clearly understood.

In part, internal audit's ability to communicate hinges on its relationships outside the audit function. Without strong relationships, even the best messaging and insights can fail to reach the intended audience, or fall on deaf ears. Internal auditors need to invest in relationships, making every effort to get to know their clients. We cannot be content merely to sit in our offices or meeting rooms with audit peers—we must venture into the business areas and talk to those we serve in the organization. We should take every opportunity to communicate not only on a formal basis but also informally—especially with key stakeholders—to learn about new or changing developments. Having breakfast, lunch, or even just a cup of coffee with senior leaders or business-unit managers can be an excellent starting point for ensuring our voice is heard.

Of course, effective communication not only requires us to be adept at sharing information—we must also listen carefully to what our clients say. Recognizing the importance of this skill, more than 90 percent of respondents from The IIA's 2016 North American Pulse of Internal Audit survey say their audit function factors active listening into its training or recruiting efforts.

We must listen "between the lines" to hear core messages. A good listener truly understands what the client says and helps assure that his or her message is received. Practitioners who possess this skill improve the quality of audit information gathering, as well as enhance the audit function's image as a reliable partner that recognizes the concerns and priorities of the organization.

ADOPT AN INTEGRATED MINDSET

Integrated auditors possess an array of competencies. While a traditional accounting or finance background is certainly valuable to the audit function, there are many other abilities that enable us to address the risks affecting our organizations.

Cyber breaches and privacy/information security issues continue to plague organizations of all types. As recent global surveys demonstrate, cyberrisk is a top-of-mind risk for boards and management; together with the rapid speed of disruptive innovation of new technologies, these are major challenges for internal auditors today and are increasingly on our stakeholders' radar. The question for internal auditors is whether we have the technical knowledge to assess and address these types of emerging risks. We must continually invest in broader IT knowledge to meet the expectations of our key stakeholders and to ensure an integrated skill set. One pathway will be through intensive training to build a solid foundation within the audit team. Beyond engaging IT auditors, there is a need

PATH TO CHAIRMANSHIP

2009	Member, IIA-Austria Board of Directors
2010	President, IIA-Austria; Member, IIA Professional Certifications Board
2012	Member, ECIIA Management Board
2013	Treasurer, IIA Global Board of Directors
2014	Senior Vice President, ECIIA; IIA Vice Chairman of the Board-Professional Guidance
2015	Senior Vice Chairman, IIA Global Board of Directors
2016	Chairman, IIA Global Board of Directors

"Auditors who see their work through the lens of multiple perspectives will be much better able to appreciate the big picture, providing a valuable asset to the organization."

THE GLOBAL BOARD

As 2016-2017 global IIA chairman, I plan to work diligently with my fellow senior volunteers in supporting The Institute's long-term strategic plan, helping to ensure internal audit professionals will be universally recognized as indispensable to effective governance, risk management, and control. That goal involves five main components:

Professionalism The IIA will lead the profession through the development of timely and relevant knowledge, global guidance, and career path guidelines.

Advocacy The IIA will raise the profile of, and demand for, the profession to ensure it is recognized as an indispensable resource by key stakeholders.

IIA as Leader The IIA will be recognized as the leading voice for internal auditing.

Capacity The IIA will collaborate globally to expand the capacity of the profession.

Sustainable Value The IIA will deploy both financial and business models that generate sustainable value for members.

I look forward to helping The Institute guide this plan from vision to reality, and to steering our profession toward increased relevance and influence in the future.

for basic or even higher levels of IT knowledge for every internal auditor. However, for some audits or investigations in the IT area, organizations will continue to need to outsource the relevant IT knowledge from an external provider.

Applying soft skills can be just as important to our success as technical abilities—perhaps even more so. Integrated auditors can, for example, navigate the political climate of the organization skillfully and approach problems with a focus on solving them through compromise. They are effective negotiators dedicated to finding common solutions for the well-being of all stakeholders.

Approaching our work with an expanded frame of reference involves not just skill sets, but a way of thinking—an integrated mindset. Auditors who see their work through the lens of multiple perspectives will be much better able to appreciate the big picture, providing a valuable asset to the organization. This holistic view, in turn, will be reflected in our primary work product, the audit report, and in our advisory services. Audit work looks

TO COMMENT on this article, EMAIL the author at angela.witzany@theiia.org

Communication is key. Witzany meets with Sparkassen Versicherung AG Board member Manfred Bartalszky (center) and Manfred Rapf, chief financial officer.

MORE

VISIT our Mobile app + InternalAuditor.org to see a video of Angela Witzany discussing her chairman's theme, "Audit Never Sleeps."

much different, and offers less value, when produced from a myopic, one-dimensional point of view.

Of course, no individual practitioner can possess comprehensive audit skills—and that's where integrated auditing applies to the whole team. Collectively, audit groups need the right people with the right backgrounds and skills. Moreover, they need to work closely and cooperatively, with great emphasis on information sharing, to enhance the team's ability to leverage integration. Having the right mixture of practitioners in the audit function, and integrating team input effectively, builds a solid basis for success.

DO THE RIGHT THING

Our work also must be guided by a strong focus on ethics. But ethical behavior involves much more than just adhering to rules or standards—practitioners must conduct audits with transparency. The audit process should always be clear and precise, well-documented with traceable evidence, delivered with sound judgment and assessments, and truthful.

Building a foundation of transparency takes time. It requires continual communication with stakeholders and working extensively to educate them on the audit process. Moreover, it involves recognizing that transparency goes beyond conducting our work in an honest manner. In other words, someone can be honest without necessarily demonstrating transparency. We need to be clear in our intentions and show precisely how our work adds value to the organization. And we must do this on an ongoing basis, with every client interaction.

Ethical behavior also means acting with integrity. Practitioners need to demonstrate soundness of character, professionalism, and respect for clients. We need to adhere to The IIA's Code of Ethics and maintain the highest standards of behavior at all times. By modeling integrity, we can have an influence on ethical conduct beyond the audit function, setting an example for the rest of the organization. Internal auditors should be the standard bearers for ethical practice.

BE STRATEGIC

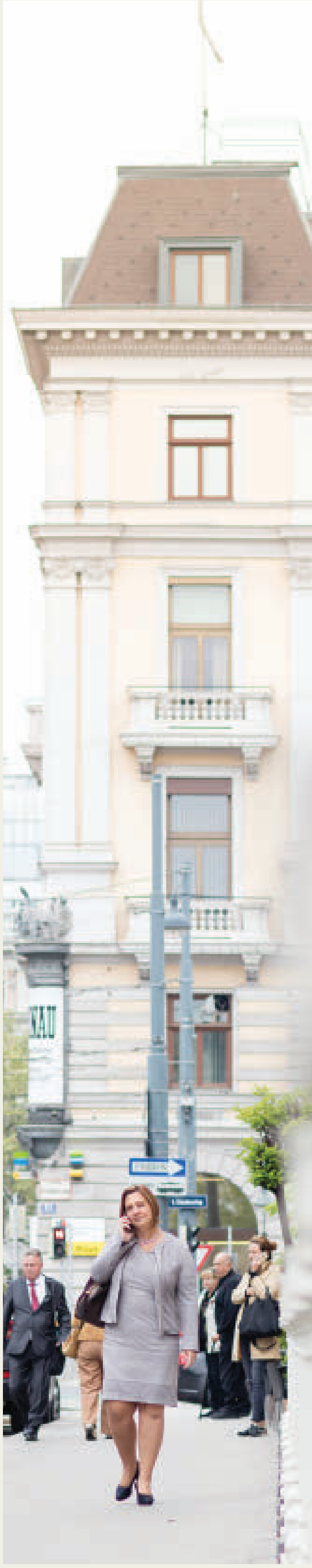
Auditors also need to approach their work with a strategic focus. Yet according to The IIA Research Foundation's most recent Internal Audit Common Body of Knowledge study, 43 percent of audit plans are not well-aligned with organizational strategy. This finding represents a significant improvement opportunity for the profession.

Remedying any deficiencies in our strategic alignment requires focused effort. It is our responsibility to ask about the organization's strategy and to make sure we understand it. For example, the CAE can ask to participate in organizational strategy sessions—even if only as a guest without voting rights—to hear what's being discussed. Alternatively, he or she could simply obtain the minutes from those sessions if in-person attendance is not feasible.

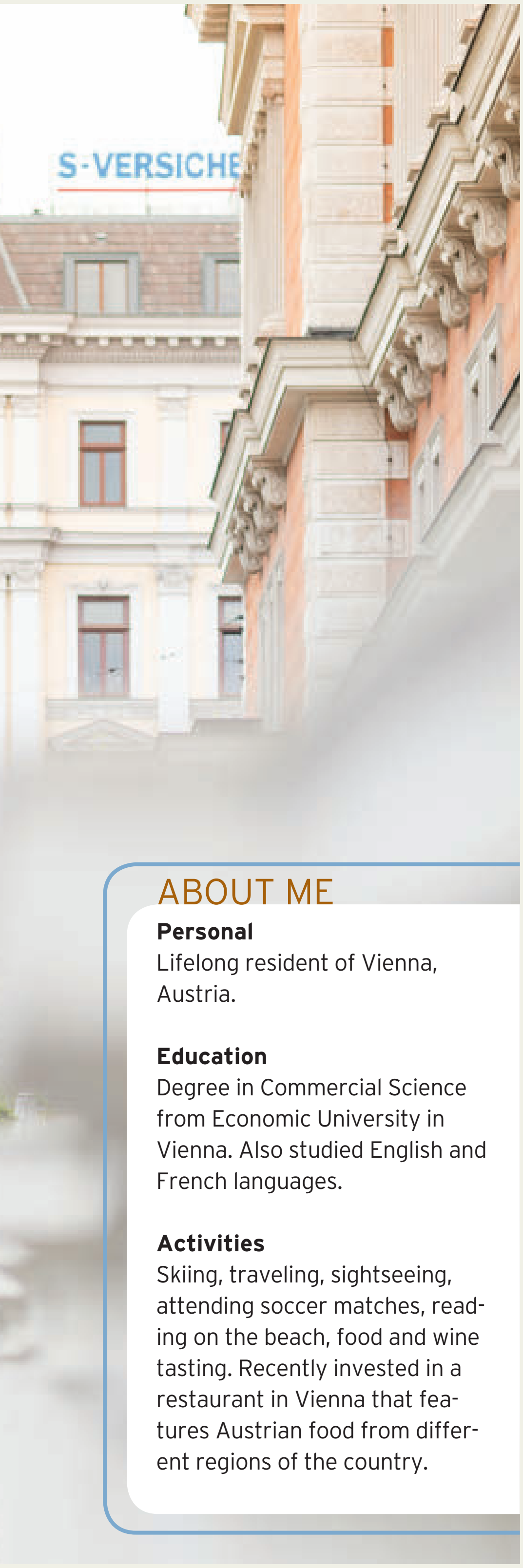
Without an understanding of organizational strategy, audit work can only be performed blindly, leaving practitioners disconnected from the work of the organization. The entire audit team needs to be aware of the strategy, as it will help inform their day-to-day work with clients.

FOCUS ON THE FUTURE

In tandem with our strategic sensibility, internal auditors must be able to anticipate what's coming down the pike. Historically, our profession has focused on the events of the past—we would determine what mistakes were made and help the organization avoid repeating them. But today, much more is required.



"We need to work tirelessly and passionately in our pursuit of excellence, and we must be ever-vigilant in finding opportunities to add value."



ABOUT ME

Personal
Lifelong resident of Vienna, Austria.

Education
Degree in Commercial Science from Economic University in Vienna. Also studied English and French languages.

Activities
Skiing, traveling, sightseeing, attending soccer matches, reading on the beach, food and wine tasting. Recently invested in a restaurant in Vienna that features Austrian food from different regions of the country.

We need to consider key risks our organizations may face and share these perspectives with stakeholders. That way, our clients can better prepare for those challenges, or opportunities, before they materialize. Looking ahead enables us to warn of pending disasters stemming from insufficient attention to business risks, or leverage new growth opportunities that may have escaped management's radar.

Internal auditors must proactively seek out information that will help them understand what lies ahead. Finding opportunities to interact with the board and management to assess their concerns and priorities is an important part of that process. Within industries that face steep regulatory challenges, auditors also should maintain good relationships with regulators to obtain a sense of what's to come in the way of requirements.

Internal auditors can often further gauge upcoming regulations, and stay abreast of other issues on the horizon, by exchanging knowledge with industry peers. I meet with other insurance industry CAEs, for example, two to three times each year to share information and best practices. At our last meeting, we discussed how new regulations like the European Union's Solvency II Directive impact our strategy as an internal audit department and our day-to-day work. These meetings keep me apprised of upcoming issues and help me add value to the organization's risk management process.

Practitioners at all levels of the audit function need to stay attuned to what's on the horizon through their work with individual business areas. During my audit team's weekly meetings, we share knowledge obtained through client interactions to ensure we collectively have a better understanding of current and future undertakings. We also place considerable emphasis on audit training—another key to remaining future focused. Training should not be sporadic—it should consist of ongoing, continuous learning. Knowledge of the latest trends affecting internal audit gives us visibility regarding what's to come and better equips us to provide the foresight our stakeholders require.

RISE TO THE CHALLENGE

In 2015, The IIA released a revised version of its International Professional Practices Framework, aimed at helping practitioners navigate through change and ever-growing business challenges. As a member of the task force that helped develop the revision, I strongly believe in the framework's Mission Statement for the profession: "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." Simply put, it is our responsibility to shape the perception of internal audit and to elevate the profession to an even higher level.

Throughout my chairmanship, I want to share my own views, experiences, and challenges. But I would like to hear from you, as well. There are numerous, diverse pathways to achieving our mission. Regardless of your career level, department size, or industry, it is my personal goal to listen to internal auditors around the world and obtain a range of views on the profession.

We need to work tirelessly and passionately in our pursuit of excellence, and we must be ever-vigilant in finding opportunities to add value. Together, we can raise the bar for internal audit and ensure the continued relevance of our profession. I look forward to hearing your stories and to sharing this journey with each of you.

ANGELA WITZANY, CIA, QIAL, CRMA, *is head of internal audit at Sparkassen Versicherung AG in Vienna.*

AHIA 35TH ANNUAL CONFERENCE
Come on Down to Georgia with Healthcare Audit on Your Mind
Georgia
ATLANTA, GEORGIA
SEPTEMBER 11-14, 2016 · ATLANTA MARRIOTT MARQUIS

Optimizing Internal Audit

Internal auditors are being continually challenged to improve their effectiveness to better meet growing expectations and workloads.

Jonathan Ngah

After ramping up investments and hiring during the mid-2000 global economic boom, organizations across various sectors rapidly implemented sweeping cost-cutting initiatives when the global recession began in 2008. Headcount reductions and high unemployment rates dominated business headlines in the U.S., with major budget cuts across functional areas, all while organizations were still expected to meet customer needs and execute their missions.

Internal audit's objective of creating value remained the same during the subsequent recovery, even as continuous budget cuts across business functions became the new normal. Internal audit departments, as well as other business units, had to adapt and find innovative ways to continuously create value for their organizations with fewer resources.

According to The IIA's 2016 North American Pulse of Internal Audit: Time to Move Out of the Comfort Zone, approximately 71 percent of CAEs reported that internal audit staffing levels are staying the same, and 25 percent indicated they will increase. This data could confirm the importance of the internal audit function, but might not necessarily address the increased workload placed on internal auditors. Additionally, limited resources means internal auditors also must prioritize the competing demands of stakeholders, who have different opinions about where internal audit's focus should be.

Even while it is expected to do more with less, internal audit can continue to improve organizational effectiveness in the areas of strategic alignment, risk assessment, operational efficiencies, compliance and quality assurance, financial reporting, and responsiveness. Ultimately, priorities vary between organizations, and these areas should be continuously evaluated to create value in the context of the organization's strategic goals.

STRATEGIC ALIGNMENT

The dynamic nature of internal auditing requires practitioners to understand the core issues impacting the organizations they support, such as tone at the top, people and culture, processes, and technology. Without in-depth knowledge of the organization's strategic direction, it is difficult for internal auditors to create value and drive the required changes for the organization to effectively accomplish its goals.

Internal audit must play a critical role in assuring that organizational activities, processes, policies, and procedures align with the strategy. With the right tone at the top and support from executive leadership, internal audit can apply needed skills and broad knowledge of the organization while working collaboratively with stakeholders to ensure strategic alignment. The process should not be limited to annual or quarterly strategic sessions.

The KPMG 2015 Global Audit Committee Survey stresses that audit committees would be more efficient in their oversight roles if they have a better understanding of their organization's strategy and risks. If the issues related to strategic alignment are important to audit committees, they must be equally important to the internal audit function that the audit committees rely so heavily on.

RISK ASSESSMENT

Risk assessments relate to ongoing organizational activities, an understanding of internal audit priorities that drive annual audit plans, and information obtained and evaluated by internal auditors from interacting with stakeholders. Internal auditors must have a strong understanding of the macro- and micro-risks impacting their respective organizations.

According to The IIA's 2015 North American Pulse of Internal Audit: Navigating an Increasingly Volatile Risk Environment, at a time when geopolitical, macroeconomic, and cyber-related incidents border on the routine, the volatility of such risks places enormous pressure on internal audit functions to have the foresight needed to address these and other emerging risks to avoid damaging surprises.

An objective methodology should be used to evaluate and prioritize risks in the context of the organization's strategic direction. The process should be ongoing and provide flexibility to make timely changes as new information becomes available. A comprehensive risk assessment methodology should include mitigation strategies in the context of the organization's resources, such as:

- **People** – Human capital with specific skills and resources to implement actions required to mitigate risks.
- **Processes** – Routine and non-routine activities performed across functional areas to help organizations accomplish goals.
- **Technology** – How well the organization uses technology to achieve results.
- **Tone at the top** – A commitment from executive management that the most talented resources, optimal technologies, and processes will be focused on value-creation activities.

Internal audit functions routinely add value by identifying risks.

OPERATIONAL EFFICIENCIES

Internal auditors, armed with knowledge about the organization's strategic direction and overall risks, have the capability to apply basic operational audit principles to drive results. Recommendations for cost-effective and sustainable solutions that reflect the context of the industry and issues unique to the organization (customer needs and mission-critical activities) should be major outcomes of operational audits. Internal auditors should perform assessments to determine required training and skills across functional areas, and assess use of optimal processes and technologies in key organizational units.

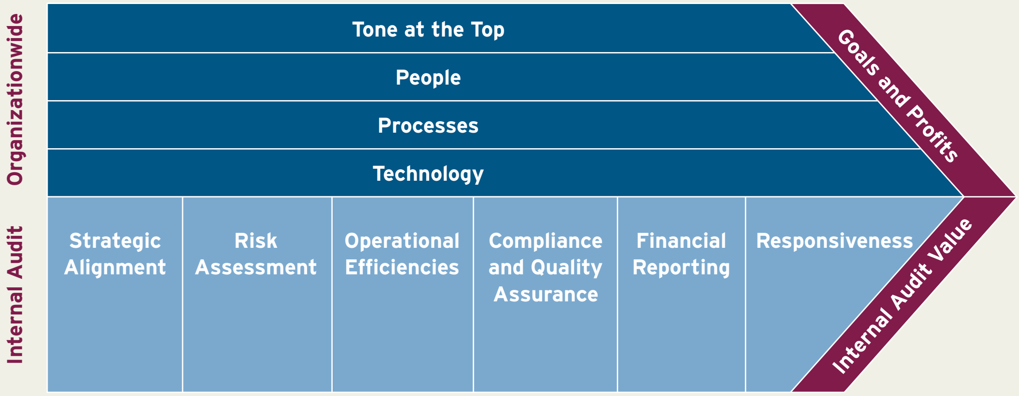
COMPLIANCE AND QUALITY ASSURANCE

Procedures to confirm important regulatory and compliance issues applicable to an organization are addressed continuously and adequately and that existing internal controls are operating

Building **strong relationships** is considered the **best strategy** for prioritizing among competing priorities, according to the CBOK Stakeholder Report, Relationships and Risk.

INTERNAL AUDIT VALUE CHAIN

Organizationwide initiatives that impact functional areas across every organization involve a combination of people, processes, technology, and tone at the top to drive accomplishment of goals and profitability. Internal audit's role requires understanding the organization's strategic direction, continuous risk management, operational efficiencies, quality and compliance, financial reporting, and responsiveness to customer and compliance/regulatory needs.



efficiently should be included in the annual internal audits and assessments.

For certain industries, the nature of products manufactured and distributed may require extra scrutiny related to quality assurance procedures (e.g., medical device companies) or added internal controls and compliance requirements (e.g., financial services companies). Internal factors such as policies, procedures, product specifications, or service levels and external factors, such as regulators and standards organizations, impact the level of effort addressing compliance.

For some organizations, quality assurance can be seen as the level of internal testing to meet product specifications. Quality compliance is the level of documentation, procedures, policies, and periodic audits to confirm the organization is meeting standards. Developing and executing audits to confirm that adequate compliance and quality assurance oversight exists in an organization and providing recommendations are examples of how internal audit functions routinely add value by identifying risks that can be mitigated or avoided before the organization suffers loss.

FINANCIAL REPORTING

For federal, state, and local government, executive managers are responsible for the stewardship and accountability of taxpayer resources and funds. The same logic applies to nonprofit organizations when funds are donated to serve a specific purpose. Private-sector organizations must implement adequate financial reporting oversight to achieve a clean audit opinion. Cost-effective financial reporting internal controls are critical for all organizations.

Internal audit plays an important role in conducting audits to confirm design and operating effectiveness of internal controls over financial reporting across enterprise operations,

ADDITIONAL WAYS INTERNAL AUDIT CREATES VALUE FOR THE ORGANIZATION

Identifying Cost Savings Internal auditors should constantly look to challenge the status quo and for ways to do things better, faster, and cheaper, without compromising the organization's ability to execute its mission, address customer needs, and maintain quality, compliance, and profitability.

Understanding Business Goals Internal auditors have the technical and interpersonal skills to encourage and support functional groups/stakeholders with often conflicting priorities to work collectively toward accomplishing organizational goals. The right tone at the top makes it possible for internal audit functions to work in an integration capacity to drive results.

Increased Collaboration Best practices and benchmarks noticed by internal auditors while working with stakeholders can be shared with other functional areas to drive organizationwide efficiencies and productivity.

Optimizing Existing Technologies Internal auditors perform various assessments to determine design and operating effectiveness of manual and automated internal controls. This includes expanded reviews and testing around significant financial and operational systems used by the organization. A byproduct of reviews performed should include recommendations for enhancements to these systems and tools.

Continuous Monitoring Working with functional managers to implement metrics and key performance indicators, as well as continuous monitoring of internal controls over critical organization operations, is key for internal audit. These includes monitoring evolving risks and potential fraud vulnerabilities impacting the organization.

Governance, Risk, and Compliance The internal audit function working in an integration capacity can save the organization valuable time and costs from performing these tasks in silos.

including IT and existence of entity-level controls. An effective internal audit function is critical in preventing and detecting material financial reporting errors, and working with stakeholders to adequately address audit findings timely. This enables external auditors to rely on work performed by internal audit and avoid duplication, resulting in cost savings.

Leveraging its knowledge of the organization's strategic alignment, customer needs, mission, risks, compliance requirements, and operations, internal audit can work with functional stakeholders to develop and monitor financial reporting metrics and key performance indicators to drive profitability. These cost-cutting initiatives to meet financial goals must never compromise an organization's ability to meet evolving customer needs and execute its mission.

RESPONSIVENESS

Ignoring audit findings or not addressing compliance issues or customer complaints may result in negative media headlines and creates public relations nightmares for many organizations. In the course of developing and executing annual audit plans, internal auditors can conduct assessments and provide recommendations to identify and correct issues before they result in embarrassing publicity.

With the right tone at the top and support from executives, internal auditors can work with functional managers in an integrated capacity to apply value creation steps in the context of each functional area and operating environment. Recommendations that are the result of working collaboratively with functional managers often lead to sustainable solutions.

Internal audit can recommend benchmarks, standardized processes, and process improvement initiatives; track return on investments; and provide input in developing and maintaining

TO COMMENT on this article,
EMAIL the author at jonathan.ngah@theiia.org

training materials. Internal auditors can provide tools to continuously monitor and prioritize risks so that corrective actions are implemented timely.

REAPING THE BENEFITS

When the internal audit function is working effectively, the organization can realize success with responsiveness to customer needs, minimal regulatory and compliance violations, productive employees, and implementation and use of optimal processes and technologies to accomplish objectives.

The internal audit function, itself, benefits from an increased perception of internal audit as a continually evolving, value-creating function throughout the organization; improved ability to understand, manage, prioritize, and mitigate risks impacting the organization; job satisfaction and improved retention rates for internal auditors working on projects that make a difference; and efficiencies gained in planning and executing future audits.

Other business units/functional areas might realize benefits, such as skills and knowledge transfer by working collaboratively with internal audit. Examples include reevaluating and improving existing practices, developing a culture of process improvement initiatives to eliminate bottlenecks and create streamlined customer-centric processes, better alignment with strategy, and increased risk awareness and mitigation techniques. Organizational benefits can include increased customer and employee satisfaction, significant cost savings, and increased productivity and profitability.

DOING MORE WITH LESS

Unrealistic demands and expectations on employees in general can have the unintended consequence of low morale, employee burnout, and reduced productivity. This is also an area where internal audit can provide options to continuously evaluate cost-saving opportunities that won't compromise its core values, the ability to execute its mission, or stakeholder priorities. Through leveraging knowledge and empowering internal audit to function in an integration capacity, auditors can help the organization accomplish its objectives while doing more with less.

JONATHAN NGAH, CIA, CISA, CGFM, CFE, *is a principal at Synergy EnterPrize LLC in King of Prussia, Pa.*

QIAL™
Qualification in Internal Audit Leadership™
SHOW THEM YOU ARE TOMORROW'S LEADER, TODAY.

BY MITCH LEE EDITED BY MARK BRINKLEY

HOW GREEN ARE WE?

Internal audit is well-positioned to provide assurance relative to sustainability rating systems.

A growing number of company executives and boards actively engaged in building sustainable and socially responsible businesses are asking this question. In fact, the escalation of interest in answering it has grown so rapidly, it has spawned an entirely new ratings industry. A recent study conducted by the Global Initiative for Sustainability Rating (GISR) identified more than 100 rating agencies and organizations worldwide offering more than 200 different sustainability rating systems. These rating systems, which cover more than 15,000 organizations, are essentially unregulated entities.

Compare that to only 10 credit rating agencies in the U.S. that cover more than 12,000 public companies across many different types of credit ratings (sovereign debt, insurance, etc.). Credit agencies are registered and certified by the U.S. Securities and Exchange Commission and are focused basically on one rating criteria: the probability that a company will default in repaying its debt in full and on time.

Answering the "just how green are we?" question has proven to be much more difficult than the question of debt repayment. Measurement of a company's environmental, social, and governance (ESG) impact is inherently a challenge. The seemingly endless number of rating criteria and approaches have created a confusing myriad of options for company leaders and boards to navigate. Selecting an appropriate sustainability rating system, however, is vital for ensuring the success of sustainability efforts. Without an appropriate measurement process in place, sustainability efforts can easily become soft and undefined, yielding minimal ESG value. Selection of an appropriate rating system can send a positive message to stakeholders as to the organization's level of commitment toward implementing sustainability practices.

As an internal assurance and consultation provider, internal audit is well-positioned to provide advice and assurance relative to the development and implementation of sustainability rating systems. There are some important principles from GISR that internal audit should consider when evaluating rating systems.

Transparency The ratings, themselves, should be accessible to those who are affected. Public access to the ratings help establish trust and credibility with multiple stakeholders. Information provided should be sufficient to meet stakeholders' needs to understand variations in results and trending patterns. The benefits of transparency,

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

TO COMMENT on this article,
EMAIL the author at mitch.lee@theiia.org

however, should be balanced with other needs of the organization, including protecting intellectual property and overall market competitiveness.

Impartiality The organization behind the rating system should be independent from undue influence, and any perception of conflict of interest should be weighed carefully during the selection process. Any commercial ties to the rating organization should be evaluated and disclosed if the potential for conflict exists.

Assurance The design of a rating system should allow for independent, third-party assurance. Even if there is not a perceived need to provide third-party assurance up front, the rating system should allow for the application of assurance activities to meet anticipated needs. Future users may seek evidence of suitable governance and oversight of the rating process to ensure data quality, accuracy, and relevance.

Materiality The rating system should be based on sustainability issues relevant to the decision-making of stakeholders. Similar to the concept of financial "materiality," sustainability materiality can change over time as the business develops. Additionally, changing scientific knowledge, shifting societal norms, and the discovery of new interrelationships require ratings to be periodically reexamined to ensure the rating system remains relevant.

Value Chain The rating system should allow for application to all portions of a company's value chain over which the company exercises significant influence. Inclusion of suppliers and third-party service providers helps ensure the credibility of the ratings and provides a holistic view of sustainability practices.

Comparability The rating system should enable users to compare the company's performance to other companies' performance over time. Comparability of evaluations of peer organizations requires a high level of uniformity and quality of data across evaluated organizations. The perception of uneven or incomplete data would undermine the ability of users to make sound comparisons. Ratings should be sufficiently explained and structured to allow users to understand the causes of significant variations among benchmarked companies.

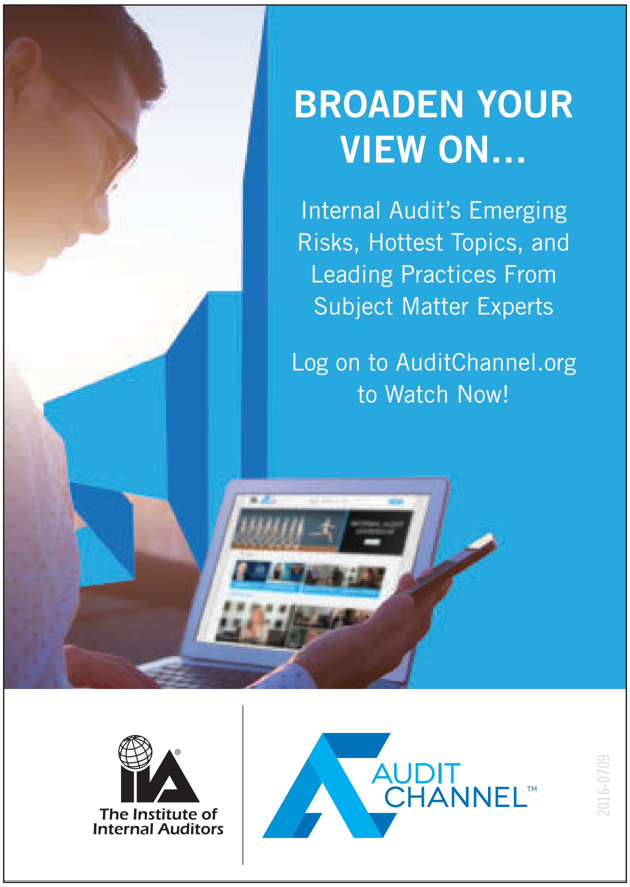
Balance The rating system should use a mix of measurement techniques to capture historical and prospective performance. Lagging and leading indicators can work in concert to provide context as to how far a company has progressed, as well as an update as to progress being made to achieve future objectives.

Collectively, these considerations, along with the needs of impacted stakeholders, can be used to select and develop a meaningful approach to rating sustainability efforts.

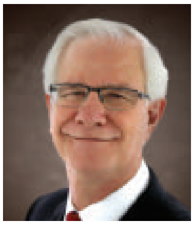
The internal and external appetite for information regarding sustainability practices is growing. Executive management and board members continue to see the benefits of pursuing mid- to long-term solutions to business problems. External stakeholders are using sustainability ratings to evaluate company performance and business resiliency. Sustainability rating systems are an important source of information for business decision-makers. The need to compare results, measure progress, and identify areas of underperformance will continue to spur the development of these systems.

As companies expand the use of nonfinancial data for external reporting purposes, the need for assurance as to the relevance and accuracy of this data will also grow. Understanding the different sustainability rating options available can help internal audit provide this much-needed assurance.

MITCH LEE, CIA, CRMA, *is internal audit director at Assurity Life Insurance Co. in Lincoln, Neb.*



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



BY J. MICHAEL JACKA

DO YOU HAVE DATA FEVER?

When it comes to gathering information, we have to remember that more is not always better.

A new internal auditor receives his latest assignment. His manager asks, "How are you going to approach the review of this area?" The auditor responds, "I want to test this, and I want to test that, and I want to test the other thing." The manager asks why the auditor wants to perform those tests. Excitedly, the auditor answers, "Because that's where all the information is."

This scenario illustrates a common mistake made by new auditors—seeking to jump in without considering the risks, the processes, the criteria, or even the audit objective. The auditor recognizes a testable area and says, "I am doing an audit of this department and I know they have expense reports, so I will test the expense reports."

Of course, those of us with years of experience and knowledge would never fall into that trap, right? Not so fast.

We live in a world where systems hold more information than anyone can possibly fathom. We are awash in data—big, large, super-sized, venti. And data analytics has become a buzzword that draws auditors like fraudsters to inadequate controls. When auditors see that glorious richness of data, they fall back into that rookie mindset: "I don't know what I want or what I'm trying to prove or what I'm going to do with it, but I want everything you've got."

At one time or another we've all caught it—data fever: The desire for more and more information without considering what that data is. We turn the fire hose on full force and what we intended to be a thirst-quenching sip of real information turns into a suffocating flood of meaningless facts, figures, and folderol.

More is not always better. The rules for gathering data are the same as for any audit test. First determine what you want to accomplish with the audit. Then articulate what you want to do with the data, coordinating that understanding with the already-identified risks.

It all begins by understanding what the data represents and what it might say. Before even thinking about asking for the data, auditors should talk with the data owners to understand what is available, how it is used, and how it relates to the processes under review. Then, and only then, should auditors begin to think about what data may be needed.

The promise of data analytics is to assist in performing audit work more efficiently. It also represents an opportunity for internal audit to provide real value by showing the organization how all that data can be helpful to everyone. But that cannot be accomplished by just gathering every scrap of data available. Just as you would stop a new auditor from barging forward with unfocused and potentially meaningless testing, stop yourself when asking for a data dump and determine what you are really trying to accomplish. 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

IT AND THE INTEGRATED AUDIT

All internal auditors need to be able to identify, and understand, the red flags associated with IT risks.

PAM JENKINS, CPA, CIA, CRMA
Vice President,
Global Audit Services
Fossil Group

TINA KIM, CIA, CGAP, CRMA
Deputy Comptroller for
State Accountability,
New York State Office
of the State Comptroller

How do you define integrated audit from an IT perspective?

KIM An integrated audit considers IT, financial, and operational controls holistically. While a traditional audit focuses on financial, operational, or IT aspects only, an integrated audit takes a more global approach. From an IT perspective, an integrated audit provides assurance that IT controls are effective and efficient to support the business process. This approach acknowledges that IT, financial, and operational controls are mutually dependent.

JENKINS There are few strategic initiatives in organizations that don't include an IT component. Our world has turned into an online world, with technology playing a role in everything we touch. The integrated audit is a more holistic approach, focused on the organization's top risks. Internal audit won't be able to present a complete picture of the organization's risks without considering the technologies associated with them.

What is your organization's approach to integrated audits?

JENKINS Fossil is a global organization with retail, distribution, wholesale, and manufacturing facilities in many countries. Internal audit aligns its audit plan with the company's top global risks. Our audit department has limited resources and IT auditors. We work efficiently and leverage our resources to ensure we address the top risks for the company. Our IT auditor is a part of every audit we perform. Over the last few months, we have begun socializing with the company a more integrated audit approach. We have the full support of the audit committee and top management. As we hire, we look for integrated auditors who can look at a business process, pick out where the risks are, and identify if there are any technology-related red flags.

KIM Integrated audits are the rule rather than exception in my organization. Organizations rely heavily on IT to perform their work. To understand an audit client's internal controls over a business process requires an understanding of the effectiveness and adequacy of IT controls. All of our staff auditors are trained to perform basic IT audits. However, for audits that are highly technical, we have a team of IT specialists with advanced IT skills. This provides us a cost-effective way to keep up with the rapid changes in technology, as well as deal with the difficulty of recruiting and retaining IT audit professionals, which can be a challenge in the current environment.

What value does a successful integrated audit approach bring to the organization?

KIM Integrated auditing promotes the principle of

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

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

risk-based auditing. The business environment is increasingly complex, and businesses and governments are confronting a wide range of risks. Integrated auditing allows audit functions to consider and evaluate risk globally and focus audit efforts on the highest impact areas. More importantly, it increases the relevance of internal auditors' work by providing better value to stakeholders. Study after study has shown that stakeholders are expecting more from internal audit functions, including those already receiving significant value. By helping to break down silos and increase transparency, integrated auditing provides management with increased insight on how various types of risks impact their business processes and gives auditors more exposure to different aspects of an organization's operation, increasing their effectiveness.

JENKINS Without an integrated audit approach, the audit results are not covering the full business process/potential risk. To ensure the largest risks of the company are addressed, the audit process needs to include IT. An integrated audit enables auditors to look at an issue holistically and identify the entire risk, not just a piece of it.

What IT skills and knowledge do internal auditors need to communicate with IT professionals?

JENKINS I think it goes both ways. Yes, audit professionals need to have comprehensive knowledge of IT to effectively identify risk and communicate with IT departments, but IT auditors also need to have more than just IT experience. They need to be able to see the forest for the trees, and communicate from a business perspective. It is important for the IT audit professional to have good business acumen to enable an understanding of the business process/risk and its relationship to the IT components. IT auditors need to bridge the gap between being highly technical and being able to speak in basic business terms.

KIM Having an education background in computer science or a related field is a big plus. However, a genuine interest and desire to understand technology, coupled with the ability to quickly grasp new trends and understand new technologies, is just as critical. Moreover, as with all audit positions, not only are technical skills important, but communication and other soft skills are also vital. To be effective, internal auditors need to speak the language of their stakeholders.

What types of IT-related audits should internal audit be able to perform without IT audit expertise?

KIM The IT audit universe represents a continuum of audit activities that run the gamut from basic to intermediate to highly technical and complex. Most internal auditors with training both in the classroom and on the job can generally progress to a level that enables them to perform a basic IT audit. In fact, one of the benefits of the integrated audit approach is that audit staff members work on a single team alongside auditors with more IT audit experience. This provides audit staff with increased exposure and experience in IT audit. That said, the continuum of IT audit activities progressively requires increasingly specialized IT skills. It is generally not cost-effective to train the entire audit team in these higher-order areas. In these instances, the use of specialists should be considered.

JENKINS Internal audit should be able to perform any broad audit with IT components. Even if the auditor is not a certified IT auditor, he or she needs to have a good understanding of where the IT risks are and be able to identify the red flags. Most audit departments do not have the bandwidth to have several auditors with deep technical skills. This is where being a part of The IIA is very helpful, because the auditors can go to The Institute for thought leadership, resources, and benchmarking to help on certain projects. We take advantage of cosourcing. These cosourcing arrangements are ideal for larger and highly technical projects that require a deeper dive into IT.

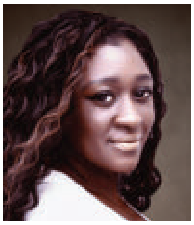
What types of IT-related audits should only be performed by IT audit specialists?

JENKINS Most audits will have an integrated approach. However, some projects may be just IT focused. It's important to be able to connect the dots back to the business side. We had our IT auditor document the organization's global IT footprint so we understand the systems in entirety and where and how they connect. We then identified where we need to drill deeper. Some of those projects may require cosourcing.

KIM The internal audit standards require that auditors have the knowledge, skills, and other competencies to perform their individual responsibilities. In the context of IT audits, these standards are uniquely challenging in that technology is constantly evolving, and, due to the costs involved, not all audit staff receive the specialized training required to keep pace. Therefore, for highly technical and complex audits involving areas such as network infrastructure or emerging technology, it is better to rely on an IT audit specialist who possesses the knowledge level and skills to meet the audit needs.

That said, recruiting and retaining such specialists is perhaps one of the greatest challenges facing audit functions that want to adopt integrated auditing. When internal resources are not available, alternatives to be considered include guest auditors or cosourcing. While the difficulties can appear daunting, the benefits in increasing risk coverage and creating efficiencies within the audit team are well worth the effort. Ia

TO COMMENT on this article, EMAIL the author at carolyn.jackson@theiia.org



BY CAROLYN JACKSON

READING BETWEEN THE LINES

Sometimes report metrics don't provide the full story on organizational performance.

Organizational reporting isn't always what it seems. Analyses and metrics often neglect to tell the full story, leaving readers with only a partial—and sometimes misleading—picture of the organization's performance. And while internal auditors may be uniquely attuned to the possibility of reporting flaws, accurate assessment still requires focused awareness. Practitioners need to remain vigilant when reviewing reports to be sure that the information presented matches actual results, as illustrated in one of my own experiences with a client.

Earlier in my career, I reviewed a line of business that tracked quality assurance (QA) metrics for a call center sales operation. The QA function maintained robust processes and, among other areas, monitored for policy, compliance, and customer treatment metrics. Bottom-line results were calculated, compiled on a dashboard, and ultimately reported to the organization's senior leadership. Period over period, the bottom line performed successfully, resulting in "green" indicators on metrics shared with senior leadership. But these results, while impressive, also served as a red flag—the unit's performance seemed too good to be true.

Digging deeper, I obtained detailed reporting for the year and immediately noticed a trend—several compliance-related line items within the bottom line had not shown even one month of success. The business process owners said they were aware of the situation but did not act because overall, the control point—QA monitoring results—fell within threshold. They also noted that the failures were based on very low occurrences. In other words, employees had only a small number of opportunities to act on the metric, and any defects that occurred would create a more exaggerated error rate. When pressed, the process owners confessed they did not have a plan to address the problem. The troubling sequence of discoveries prompted action.

Following the audit, a work group that included the organization's three lines of defense collaborated to revamp the QA tracking processes. The new system identified lower opportunity metrics and tracked them in a separate category, using a per-unit scale instead of a defect percentage rate. These changes enabled the business line to track its compliance metrics' true performance and address issues more effectively.

As far as I could tell, the unit's deficiencies resulted from ambiguity and negligible indifference rather than intentional manipulation. Nonetheless, the lessons learned apply to both fraud- and error-related circumstances. All too often, bottom lines that aggregate results into an average or ratio tend to ignore the smaller, nonperforming components that could be missed period over period and fester into larger issues. Internal auditors need to remain alert to the details at all times and read between the lines on reports where the business might be too focused on bottom-line results. Ia

CAROLYN JACKSON, CRMA, CCSA, *is a senior audit manager at Capital One in Plano, Texas.*

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

2016 ALL STAR CONFERENCE

Oct. 17–19, 2016 / Las Vegas, NV

EXPERIENCE THE BEST OF THE BEST!

Connect with the highest rated presenters from the past year of IIA educational programs, enjoy an exciting new session format, and leverage learnings from a wide variety of transformative sessions.

- Go beyond processes and controls to explore the essential role internal audit can play.
- Identify enterprisewide business efficiencies.
- Gain strategic insights that improve business performance.
- Focus on discerning the risks that matter to your organization.
- Earn up to 16 CPE credits.

IIA Members, register by Aug. 17 to **save US$200**!

New! Keynote Speaker

Ed Robinson

Chief Executive Officer
Rainmaker Performance Group

Leveraging Millennials to Win the Leadership Race

Register today!
www.theiia.org/AllStar

The Institute of Internal Auditors

2016-2192

Wolters Kluwer

When you have to be right

The Millennial Auditor

Is your department prepared with the flexibility, policies, and technology to attract and manage the next generation of auditors?

flexibility

policies

technology

IIA PRINCIPAL PARTNER

Read Our Latest Report to Learn How:
TeamMateSolutions.com/Millennials