Ia
INTERNAL AUDITOR

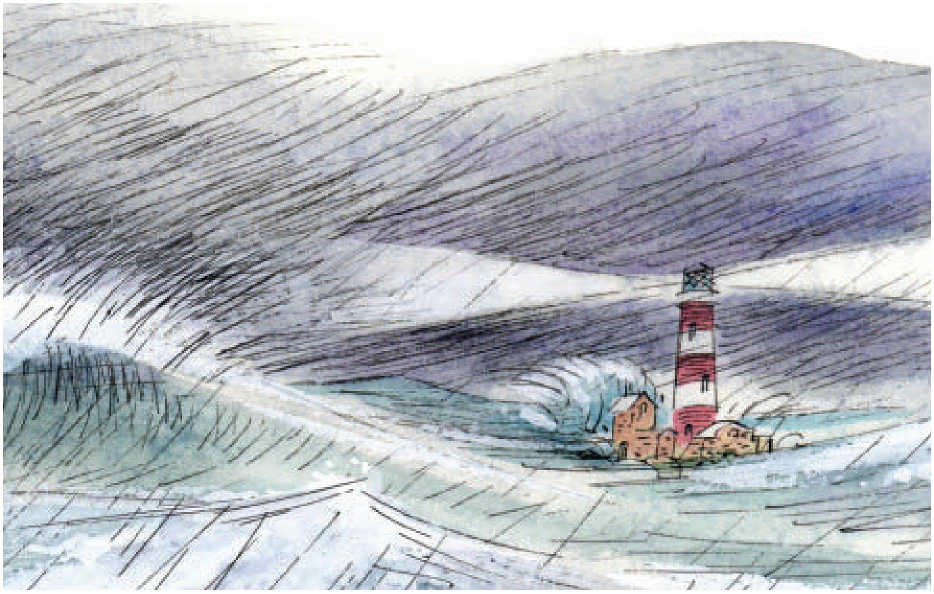
APRIL 2017 INTERNALAUDITOR.ORG

RESILIENCE THROUGH CRISIS

As a key steward of organizational well-being, internal audit can play an active role in making resiliency a part of all operations.

Ia
INTERNAL AUDITOR

APRIL 2017 VOLUME LXXIV: II



FEATURES

Ia

INTERNAL AUDITOR

APRIL 2017 VOLUME LXXIV: II

DEPARTMENTS

ONLINE InternalAuditor.org

In High Demand A new IIA/Robert Half report finds that well-qualified internal auditors are highly sought after – and generously compensated.

Pulse of the Profession
Watch a rundown of findings from The IIA's 2017 North American Pulse of Internal Audit survey.

In the Wrong
Fraud expert Art Stewart discusses a rare case of a company admitting to wrongdoing in a U.S. securities case.

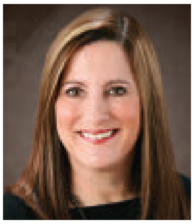
The Dark Side of IoT
Cybersecurity professionals warn of rising attacks on internet-connected devices.

Find us on Facebook

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: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A.

Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Lake Mary, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001.

IMAGES: COVER, VADYTHEHERA (CLOUD ICON); TOP, IGORSTEVANOVIC / SHUTTERSTOCK.COM; RIGHT, RETROROCKET / SHUTTERSTOCK.COM



WHEN THREATS BECOME REALITY

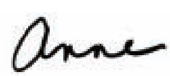
Cyberattacks and data breaches are once again the top two threats to business continuity in 2017, according to the latest Horizon Scan Report, published by the Business Continuity Institute in association with the British Standards Institute. Nearly 90 percent of the 726 responding organizations from 79 countries report they are concerned about the possibility of a cyberattack, while 81 percent of respondents say the same about a data breach. According to the report, the eight other top threats are: unplanned IT and telecom outages, security incidents, adverse weather, interruption to utility supply, acts of terrorism, supply chain disruption, availability of key skills, and new laws or regulations.

Such threats can test an organization's resiliency. *Risk Management* magazine recently presented a list of 30 actual risk events that occurred last year. The "Year in Risk 2016" shows how broad the spectrum of threats is. For example:

- A massive denial of service attack blocks access to dozens of websites, including Reddit, Twitter, Amazon, and Netflix. The hacker's identity is still unknown.
- The U.S. federal government declares a state of emergency in Flint, Mich., after unsafe lead levels are found in the water supply. Five local and state government officials resign or are fired, and criminal charges are filed against nine others.
- Following foodborne illness outbreaks at Chipotle Mexican Grill that sickened hundreds of customers, sales are down and the restaurant's stock price has dropped nearly 50 percent since its August 2015 peak.
- Terrorist attacks kill more than 340 people in a shopping center bombing in Baghdad; 87 people in the Bastille Day massacre in Nice, France; 49 people in a nightclub shooting in Orlando, Fla.; and 35 people in a train station bombing in Brussels—sadly, to name just a few.
- In June, 52 percent of U.K. voters elect to leave the European Union. It is yet to be seen how Brexit will affect commerce and trade.

Business resiliency is all about the organization's ability to quickly adapt to risk events such as these while maintaining continuous operations and safeguarding its employees, assets, and brand equity. In this month's cover story, "Resilience Through Crisis," author Mike Jacka takes a comprehensive look at internal audit's role in business resiliency—from crisis plan development, to plan implementation, to post-crisis analysis. In a world full of risk, internal audit can take a proactive role in organizational well-being.

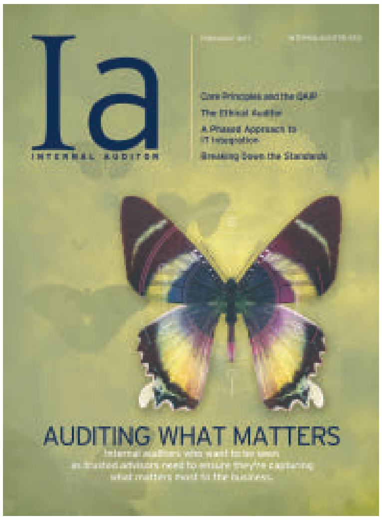
On a separate note, welcome to Charlie Wright, our new "Risk Watch" contributing editor. Wright is director, Enterprise Risk Solutions, for BKD LLP in Oklahoma City. He replaces Paul Sobel, who has contributed his time and expertise to the department since 2008. Thank you, Charlie and Paul!



@AMillage on Twitter

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.



Ensuring Credibility

It is absolutely true that "If internal audit wants to ensure true credibility with its stakeholders, we must look inward." The report preparation and review process does take a lot of time. But, this is the one tangible product that we deliver (for the auditees, board members, our peers, etc.). So it's important to get it right. My senior manager says that workpapers can be perfect, ticking and tying down to the penny and explaining the process and players thoroughly, but if the report is inaccurate, it doesn't matter. At the same time, it's important to be efficient.

Before I get too heavy into preparing a report, I look at similar findings from past reports and institutions to see if prior wording/terminology can be used to achieve all of the elements of the finding and recommendation I am writing for the current report. It's also good to have a peer who has worked with a manager or institution before, and can anticipate questions, do a quick review of your draft report.

SYED OWAIS RIZVI *comments on Mike Jacka's "The Beam in Internal Audit's Eye" ("The Mind of Jacka," February 2017).*

Collective Unease

I must say, you wrote this blog post at the right time. Currently, all across the globe, there is lots of confusion and feelings of uncertainty due to President Trump's policies. This is definitely shaking the confidence of internal auditors everywhere.

BHALCHANDRA BALSHETWAR *comments on the Chambers on the Profession blog post, "What Will the Trump Era Mean for Internal Auditors?"*

Embedding Compliance

This is an excellent article. I am currently building an internal audit department. I plan to use this guidance in establishing the function, so compliance is embedded in the design with no additional compliance efforts required over and above what we define with management and the board. Additionally, I am considering having a quality assessment benchmark performed by The Institute after the first year to make sure we are on course, rather than waiting to do it in year five.

THOMAS BISHOP *comments on Christine Hovious' "Breaking Down the Standards" (February 2017).*

Falling Asleep at the Wheel

NCI is one of many government contractors where there are flaws or weaknesses in their financial management systems. The interesting part is that the awarding agency, in most cases, falls asleep at the wheel of enforcement of the requirements regarding the establishment of an

Ia INTERNAL AUDITOR
APRIL 2017
VOLUME LXXIV:II

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

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")

effective financial management system. From my experience, both the government agency and contractor have the mentality that as long as the project or service is provided, who cares? This mentality needs to change because fraud, waste, and abuse tend to follow.

FREDERICK LEE *comments on Art Stewart's "The Out of Control Contractor" (InternalAuditor.org, February 2017).*

Balancing Act

Just the definitions of *fact* and *truth* are very challenging to communicate because most people aren't familiar with how to construct a logical argument. Auditors naturally prepare a list of facts (statements) and then make recommendations (claims, opinions, or conclusions). The factual statements should not be in dispute, although the recommendations may have lively debate with smart people disagreeing.

A fact can be independently verified and everyone should be able to agree on it. It merely exists and should not be conflated with "truth" as you said. If there is a dispute, it isn't a fact, it's something else.

In sum, either a fact exists or it doesn't. Opinions are either true or false, but we don't always know for sure. Facts and opinions have to be stated very precisely to allow evaluation. As the late-great Daniel Patrick Moynhan is reputed to have said, "You are entitled to your own opinion. But you are not entitled to your own facts."

FARCASTER *comments on the Chambers on the Profession blog post, "There Is No Room for Fake News or Alternative Facts in Internal Audits."*

MORE

VISIT InternalAuditor.org and click on the Voices section to read the latest blogs and leave your comments.

Who Are Internal Auditing's Future Leaders?

What defines an **extraordinary** internal auditor?

Innovation, integrity, knowledge, and passion, among other qualities. Do you know a high-performing internal auditor who possesses the traits to become tomorrow's thought leader? Acknowledge their dedication and nominate them today.

Internal Auditor magazine will recognize up-and-coming internal audit professionals in its annual "Emerging Leaders" article in October.

Nominate by May 12, 2017, at **www.InternalAuditor.org.**

2017-0305

Disclosing anti-corruption data... Pulse report highlights overlooked risks... The risk of acting on fake news... Corporate cyber risk defenses down.

Update

BRAND DAMAGE PAIN

Reputation loss can be an ongoing, unpredictable risk to address.

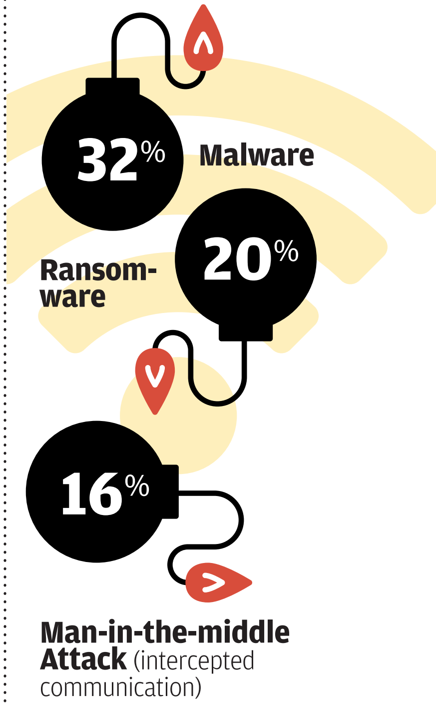
Organizations most fear damage to their brand (63 percent) as a result of having a nonexistent or poorly executed risk management program, according to The Imperative to Raise Enterprise Risk Intelligence, a recent survey conducted by the Ponemon Institute and sponsored by RiskVision, an enterprise risk intelligence company. Following brand damage are security breaches (51 percent), business disruption (51 percent), and intellectual property loss (37 percent).

"Expenses around compliance, customer attrition, and negative public relations incurred due to resulting loss of brand and reputation are ongoing, sometimes dragged out for months or even years, and are much more difficult, if not almost impossible, to predict or gauge," Larry Ponemon, chairman and founder of the Ponemon Institute, says. "While security breaches are costly to detect and remediate, the costs are finite."

Of the 641 individuals involved in risk management activities who were surveyed, 83 percent say managing risk is a significant commitment for them. However, three-fourths of organizations lack a clearly defined risk management strategy or they have one that isn't applicable to the entire organization. This represents a disconnect in organizations' desired risk practices and

OBJECTS OF MALICE

Three common attacks targeted internet-connected devices in 2016.



Source: Pwnie Express, The Internet of Evil Things report

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

IMAGES: TOP, IGORSTEVANOVIC /SHUTTERSTOCK.COM; RIGHT, MAYRUM (BOMBS) AND TELMAN BAGIROV (WI-FI ICON) / SHUTTERSTOCK.COM

VISIT InternalAuditor.org to view a video about the 2017 North American Pulse of Internal Audit Report.

what they can realistically achieve. Other key report findings include:

- » Only 14 percent of respondents say their organization's risk management process is effective.
- » Just over half of organizations don't have a budget for enterprise risk management.
- » The top three barriers to achieving risk management goals are lack of resources (44 percent), complexity (44 percent), and the inability to get started (43 percent).

The report also notes that raising enterprise risk intelligence can be achieved by breaking down silos and encouraging collaboration. Fifty-three percent of respondents say finance, operations, compliance, legal, and IT operate in silos when it comes to managing risk. **—S. STEFFEE**

Fraud costs U.K. businesses an estimated

£125 billion

(US$155 billion) annually, with average losses up 43% since the 2008 start of the worldwide recession.

Globally, the US$4.39 trillion estimated financial cost of fraud is

2/3 greater

than the U.K.'s gross domestic product.

"In every sector in every country, fraud has a serious and detrimental impact on the quality of life," says Jim Gee, partner and head of Forensic and Counter Fraud Services at advisory firm Crowe Clark Whitehill LLP.

Source: Crowe Clark Whitehill and the University of Portsmouth Centre for Counter Fraud Studies, The Financial Cost of Fraud 2017.

ANTI-CORRUPTION DATA REMAINS UNDISCLOSED

Countries are keeping financial crime data to themselves.

Global anti-corruption watchdog Transparency International (TI) says in a new report that bank regulators need to publish more information about banks' compliance with anti-money laundering laws. Sharing this data would give citizens and businesses confidence that corrupt individuals and organizations do not use the global banking system, TI concludes.

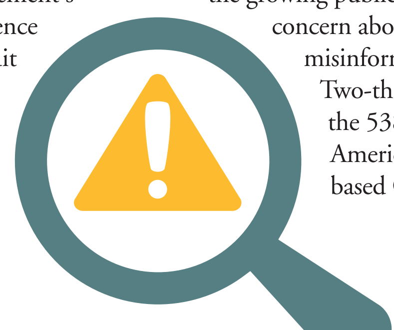
The report, Top Secret, shows that information about authorities' anti-money laundering efforts is only partially available across the 12 countries assessed. Only four countries publish the total number of sanctions applied to banks for money laundering failures, and only two provide information about anti-money laundering extradition requests. Across all 12 countries, just over one-third of anti-money laundering indicators are disclosed fully.

"Mistrust of banks will continue unless people know they are working on their behalf and not for the corrupt," says TI Chair José Ugaz. **—D. SALIERNO**

FOUR RISK AREAS IN FOCUS

Pulse report sees opportunity in auditing overlooked risks.

Chief audit executives (CAEs) could boost management's confidence in internal audit by filling an assurance void in often-overlooked areas, notes the 2017 North American Pulse of Internal Audit report from The IIA's Audit Executive Center.



One of those overlooked areas dovetails with the growing public concern about misinformation. Two-thirds of the 538 North America-based CAEs, internal audit directors, and senior audit managers who responded to the survey say communicating errors and other misinformation about company performance through channels other than financial reports is a high risk to their organization. Yet, just 9 percent say their audit function covers this risk in their audit plan, according to the report.

IMAGES: TOP, XTOCK / SHUTTERSTOCK.COM; RIGHT, VICTOR TONDEE / SHUTTERSTOCK.COM; LEFT, NOBELUS / SHUTTERSTOCK.COM

Another costly risk area is environmental, health, and safety (EHS), the source of more than US$13 billion in federal government fines for U.S. organizations in 2015. Despite such potential costs, only 48 percent of respondents say they include EHS risks in their audit plan. Boards and audit committees are more likely to receive such assurance from the risk management or compliance functions, or from a specialist EHS audit function.

CAEs should find the courage to take on these and other risks, the report advises. "Courage is a character trait many top audit leaders exhibit, not just in dealing with the pressures inherent to the job, but also in addressing areas that may be taboo or historically overlooked," says IIA President and CEO Richard Chambers.

One area where some internal audit functions have been forward-thinking is data analytics. More than 40 percent of respondents say their internal audit department always or frequently uses data analytics in its audits.

On the other hand, interpersonal communication tests many CAEs' resolve. Thirty-six percent of respondents say negative interpersonal exchanges with others in their organization happen sometimes or frequently. Among those respondents, 35 percent say such exchanges would affect the ability to conduct an audit. **— T. MCCOLLUM**

THE AGE OF MISINFORMATION

Being able to trust an information source is critical to decision-making, says Todd Bialick, PricewaterhouseCoopers' trust and transparency leader.

What risks do fake news and misinformation create for organizations? The volume of information available to organizations increases the risk of some of that information being inaccurate or incomplete. While it can't be assumed that all information is wrong, better measures need to be taken to verify it when making important management decisions. Trusting the source of information, and being able to show that it is verifiably accurate, is critical to effective decision-making. Acting on misinformation can inhibit the organization's ability to not only effectively execute on its strategy, but also could lead to potential compliance-related issues.

How can organizations verify that they're not acting on misinformation? Developing a formal approach to verifying data and information is key to helping organizations make better-informed decisions. Whether information is coming from traditional media, social media, third-party vendors, or customers, aggregating and triangulating all of the data sources using dashboards and visualization tools that pull from different traditional inputs and structured and unstructured data sets can allow businesses to make more informed decisions. Social scanning and customer feedback are other ways that organizations can better position themselves to interpret information, assess its accuracy, and respond quickly to issues.

MORE

VISIT InternalAuditor.org to read an extended interview with Todd Bialick.

COMPANIES OFF GUARD

FTSE 100 firms anticipate cyber risk, but keep their defenses down.

Although most U.K. FTSE 100 companies identify cyber risk as a principal risk in their annual reports, few are preparing for such threats, according to Deloitte's analysis, Cyber Risk Reporting in the U.K. That lack of readiness is glaring at the top, where only 10 percent of companies delivered cyber risk training to their board last year. Just 5 percent have a director with technology or cybersecurity experience.

"The time is coming when boards will want greater expertise and experience around the table for specialist areas such as technology," says Deloitte Vice-chairman William Touche in the report.

Beyond the boardroom, 27 percent of companies identified a person or team that is responsible for cybersecurity, and 5 percent have insurance against cyber risk. Most companies disclosed that they have cyber contingency, crisis management, or disaster recovery plans, but only 58 percent say they have tested these plans. **— CLAUDIA GESIOTTO**

PHOTO: RIGHT, JOE PRACHATREE / SHUTTERSTOCK.COM

BY CHRISTINE HOGAN HAYES EDITED BY JAMES ROTH + LAURA SOILEAU

WORK SMARTER, NOT HARDER

Managers can use a framework to help guide employees toward more productive work and improved communication.

The phrase "work smarter, not harder" encourages an increase in productivity and efficiency. It can motivate an employee to identify the most important and necessary tasks and execute them with accuracy and completeness while eliminating from one's day the unnecessary activities that add no value.

But without action steps to work smarter, the phrase lacks substance. Through the identification of the root cause, a manager can devise a specific solution to the barriers the employee is facing and possibly eliminate such roadblocks. The following framework can support the struggling employee and identify the root cause of the problem, strengthen the employee/manager relationship, encourage thoughtful and honest conversation, and promote collaboration between the two parties to identify relevant solutions. The framework may also positively impact other auditors in the department, as well as departmental stakeholders.

Acknowledge the problem

If an employee has been behind and missing deadlines or has been putting in long hours, it is time to come to an agreement that he or she is experiencing a roadblock and his or her current approach is not sustainable for the long term (i.e., burnout). At this stage, validation from a manager can be encouraging.

Appreciate the employee

Thanking an employee for his or her hard work can be meaningful. Recognition of the time and effort already expended helps promote a constructive dialogue. The long hours may be indicative of an employee who cares about his or her work product, but may not know the best way to get that valuable work product completed. An employee who displays this level of dedication is one the department wants to retain.

Identify the root cause

Though an employee may be able to define the problem, there may be other obstacles at play that he or she is not defining as obstacles. The employee should walk through a typical day—or week—with his or her manager to determine which tasks and activities the employee is completing and not completing. This conversation should be treated like a typical internal audit walk-through, with a thoughtful mix of open-ended and closed-ended questions, such as:

- What deliverables is he or she producing?
- What is he or she requested to perform?
- What is the estimated time it takes to complete each task? For example, if

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

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

an employee is a junior- or entry-level associate, the demands and pressures placed on him or her by the senior or supervising auditor while on an engagement may be enlightening—and surprising.

Define the roadblock After discussing a typical day or week, the employee's responsibilities, challenges, and habits should become more clear. At this point, it may be possible to identify what is holding the employee back from working efficiently and productively. Ask the employee what is holding him or her back. If the response doesn't align with the manager's thoughts, continue to ask the why and how questions. Once the issues are clearly identified, encourage the employee to think of them as roadblocks. Most roadblocks can eventually be cleared; for those that can't be (e.g., permanent road closure), there is always an effective detour (e.g., a reasonable and realistic solution).

Devise a solution Once the roadblock is defined, a solution can be determined and implemented. Three of the more common solutions are listed below. Depending on the roadblock, however, a different solution may be more effective.

- **Training**–Is this employee new to the company? Maybe he or she is confused about the company's systems or industry terminology. Is this employee new to internal audit? Maybe he or she is confused about a particular internal audit process. Connect the employee with the specific resource that can assist him or her in learning and development. The resource may be someone within internal audit, within the company, or external to the company, but should be someone who has the knowledge and can teach the skill effectively. The best option would be someone who came from a similar background as the employee (e.g., external hire), who previously experienced such a roadblock (e.g., help with the company systems), or has achieved success (e.g., a systems subject matter expert). Working with this type of mentor can provide much needed reassurance that success is attainable.
- **Resource allocation**–Has the employee taken on too much? Maybe he or she volunteered for too many projects or is performing work that is above the knowledge, skill, and experience of his or her ability? Lighten the employee's workload and frame it positively. One way is to explain to the employee which tasks are the most important. Once these tasks are completed timely and accurately (and the associated skills are mastered), other projects can be added to further develop the employee's skills. Another way to frame it positively might be for the manager to share with the employee whether he or she has been in the same situation.
- **Process improvements**–One or more of the internal audit processes may be inefficient. Sometimes new employees can see this, whereas experienced employees are accustomed to doing things a certain way and don't recognize the inefficiencies. There may be time-consuming deliverables that are either not necessary or duplicative, and there may be opportunities to improve and streamline processes.

  The solution of process improvements requires management to identify the full population of tasks that are completed within the department and evaluate whether each task is necessary and not duplicative. However, once process improvements have been implemented, it may increase not just the employee's efficiency, but that of other team members within the department.

> **By guiding employees in the direction of working smarter, it is more likely that companies will retain employees.**

Circle back Checking back in with the employee may be the most important step. Was the solution effective? How does the employee feel about the solution? Monitoring the employee's progress through regular one-on-one meetings helps to ensure that the solution is operating as intended, and it continues open lines of communication between the manager and employee. And if the solution is not operating as intended, a determination can be made for why it is not and what can be done differently.

The framework provides an outline that can support hard-working team members who may need an encouraging conversation and guidance on how to implement such a strategy. By guiding employees in the direction of working smarter, it is more likely that companies will retain employees while seeing an increase in productivity and morale.

CHRISTINE HOGAN HAYES *is a senior internal audit specialist at Plymouth Rock Management Co. of New Jersey in Red Bank.*

BY KEVIN LEUNG + JASBIR SINGH EDITED BY STEVE MAR

THE DATA MUSEUM

Internal audit can provide greater insight by compiling organizational data in structured exhibits.

VISIT Internal Auditor.org to read an expanded version of this article with examples of the CRA's SQL queries of its data museum.

More packets of data pass through the internet than there are grains of sand on the earth. Some organizations have already recognized the great potential that lies hidden within their operational and administrative data stores. For that reason, data management and data quality are among the most important considerations for business intelligence practitioners. However, practitioners must spend most of their effort on curating, cleaning, and preparing data before they can glean any meaningful information through analytics.

Increasingly, internal audit functions also are expected to use data analytics to tap into their organization's data stores. To do so, auditors need a way to understand, structure, and catalog that data so it tells a story. In the words of the movie hero, Indiana Jones, "it belongs in a museum."

Internal auditors and data analysts within the Canada Revenue Agency's (CRA's) Audit, Evaluation, and Risk Branch (AERB) are adapting data warehousing principles to create a data museum to support internal audit engagements. This database environment contains useful data curated from various sources to describe historical and current performance levels of CRA operations and administrative activities. The data museum is intended to support a wide variety of engagements at any given time, and could increase internal audit intelligence.

Internal auditors, program evaluation analysts, and risk managers will be able to browse the data museum, helping them provide more insight, oversight, and foresight for the entire organization. The data will be easily accessible in a format that is ready for analysis, and auditors will be able to browse through the relevant exhibits to gain insight into the controls they are examining.

Curating Data

In setting up a data museum, internal audit departments need dedicated "archaeologists" to discover and curate new data sources. These individuals select data sets to add to the museum based on four criteria:

- Relevance—Would the data provide information about internal controls, identifying and mitigating risk? Would it help make data-driven business decisions?
- Reliability—Is the data relatively free from integrity issues? Would it be easy to prepare the data for permanent display and use by auditors?
- Reusability—Will the data be able to support a critical mass of engagements?
- Rarity—Is the data currently unavailable in a format that is ready for immediate use?

In addition to curation, the data museum relies on thoughtful arrangement of

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

SHOUT IT OUT!

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

Download The IIA's updated Building Awareness Toolkit, featuring creative ideas, tips, tools, templates, and new information for reaching out to educators. All designed to help you promote the profession in May and throughout the year.

Mark your calendar for International Internal Audit Awareness Month: **May 2017!**

Show the world you're proud to be an internal auditor with the 2017 International Internal Audit Awareness Month celebration icon!

www.theiia.org/goto/awareness

The Institute of Internal Auditors

2017-0102

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

exhibits into themes, similar to how traditional museums are organized. Data are extracted from the CRA's data warehouse and source systems, assessed for value, and prepared and made into exhibits that are displayed by theme for internal audit use. Some data artifacts also can be reused in multiple exhibits and categorized in other themes.

If a particular engagement requires new data, which is not available, then a new exhibit can be created. If the new exhibit proves to be reusable for future engagements, then it can become part of the data museum's "permanent collection."

The HR Exhibit

One of the exhibits in the CRA's internal audit data museum contains information about all employees within the agency. The human resources (HR) exhibit is a curated set of data tables from the CRA's HR database, which was prepared and loaded into the museum. These tables include employee status, personal information, payroll, time reporting, and assignment.

In setting up the exhibit, the AERB studied the structure of each table and the relationships among them, allowing the department to automate some aspects of data preparation and maintenance. It used Microsoft SQL Server Integrated Services to extract, transform, and load the data, which is refreshed regularly. The department also continues to search for and add new artifacts to the exhibit to keep it relevant, which enables internal auditors to retrieve recent information about any employee or groups of employees.

Using SQL The fastest way to start exploring the AERB's HR exhibit is to run query statements using Structured Query Language (SQL), which selects records from the exhibit and can be exported into reports. Basic SQL statements are not difficult to formulate, and some of the department's internal auditors are already using them to browse the exhibit to access, analyze, and review its data.

Internal auditors can use the information in the HR exhibit as evidence in support of engagement observations and findings. There is also potential to uncover risks to achieving control objectives through trend analysis and data analytics.

Tools In addition to using SQL statements, there are other means to browse and analyze the HR exhibit. Because the data museum resides on a platform that supports Open Database Connectivity, auditors can connect to the data with more sophisticated analysis tools as well as import data into traditional audit tools.

For data visualization and advanced reporting, auditors can establish a direct connection to the data with Microsoft SQL Server Reporting Services. For simple reporting, auditors export the results of queries to Excel. The flexibility of the AERB's environment will also allow the department to consider using other data visualization tools.

A Horizontal View A horizontal view of an organization can be achieved by exploring the various exhibits within a data museum holistically. For example, the AERB's HR exhibit could be explored along with a financial transaction exhibit. If high-risk transactions are found within some organizational units, further analysis of HR data could determine whether there is a sufficient number of employees with various roles to achieve effective segregation of duties.

Gaining Insight

Establishing a data museum can give internal audit departments insight from the vast amounts of data within their organization. To get started, they should:

- Take stock of recent engagements and determine whether there are any frequently used domains of data, which can be formed into exhibits.
- Decide on an environment to house the museum. Choose a relational database system that will meet internal audit's needs.
- Start small. Design the first exhibit, and understand the business line and corresponding data repository. Decide which tables and data fields the department should keep.
- Learn how to write basic SQL statements. This will allow auditors to "interview" the exhibits within the data museum.
- Ensure audit trails and logs have been activated so browsing activities comply with internal security policies. Leverage this ability to validate whether management follow-up occurred.

As an integral part of the internal audit strategy, a data museum can give auditors insight into the functioning of controls, the achievement of business objectives, and the identification of risk. Information extracted from queries also can help auditors scope audit programs appropriately. Auditors can perform more sophisticated analytics on the data during the audit testing phase as well as during audit follow-up to assess whether management action plans resulted in improvements. If the data museum is visited regularly—independent of any particular engagement—then the information could be used as input into risk-based audit planning activities, helping to increase overall internal audit intelligence. Ia

KEVIN LEUNG, CIA, CPA, CMA, *is an internal auditor and data analyst at the Canada Revenue Agency in Ottawa, Ontario.*
JASBIR SINGH, CISA, *is an internal information systems auditor and data analyst at the Canada Revenue Agency.*

Risk Watch

BY BRIAN BARNIER EDITED BY CHARLIE WRIGHT

THE MANY FACETS OF RISK

Internal auditors need to consider the variety of perspectives business functions have for managing risks.

Feeding the world is the great legacy of Cyrus McCormick, whose invention of the mechanical grain reaper in 1832 was the first harvesting productivity improvement in 1,000 years. Shortening harvesting time decreased the risk of missing the narrow window for harvesting ripened grain. To grow sales, he produced reapers of higher quality than competitors. Perhaps a greater innovation was the widespread introduction of equipment financing to enable farmers to buy a reaper before they received the money from their harvest. For this, McCormick had to manage credit risk.

McCormick's innovations illustrate that risk always has been a multifaceted concern for companies, with each facet's methods refined over time. Practically every role in any organization is directly or indirectly related to risk management. Different industries and professions have long-standing methods for managing risk. To be conversant in how the organization addresses risk, internal auditors navigating today's complex and interdependent business environment must be able to understand the risk management views and calculations used by many different disciplines.

Many Perspectives

Over time, organizations have created a plethora of functions that manage business risks from their own point of view.

Product and Market Research Researchers look at risk by product or market life cycle. For example, missing customer needs, mistakes in product design, poor messaging, insufficient trial or repeat purchases, product extensions, upgrades, and delays in discontinuing a product are all risks that product managers routinely face. Mathematically, a key formula is "expected value of perfect information." Product managers are constantly asking themselves, "What is the risk (probability) of missing an insight if we don't invest more in research?" *New Products Management* by Merle Crawford and Anthony Di Benedetto is a key resource.

Strategy and Competitive Analysis Strategic professionals look at risk in stark terms—the potential of having business value diminished by failing to understand dynamics in competitors, customers, and products (including substitutions). They are constantly asking, "What am I missing?" and looking for ways to overcome structural blindness. For strategists, the risk that springs from change creates opportunity. Taking risk and managing it better than competitors is the ultimate competitive differentiator. This is illustrated by popular books such as Jim Collins' *How the Mighty Fall*, Harold Evans' *They Made America*, and Peter Diamandis' *Bold*.

SEND RISK WATCH ARTICLE IDEAS to Charlie Wright at charliewright.audit@gmail.com

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

Financial Management A central responsibility of finance is to allocate capital to the best investments. Two frequently used formulas for guiding these investment decisions are net present value (NPV) and options modeling. NPV is the more popular of the two. The numerator in the NPV formula is the risk-adjusted return of a proposed investment. The denominator is the overall or average risk-adjusted cost of capital to a business or business line. Both the proposed investment and average NPV include the time value of money. If the proposal's return is better than the average, the decision criterion is to fund the project. Options modeling extends NPV by breaking an initiative into phases. At each phase, the question is asked, "What is the probability that the value of the business options for action created by funding the initiative is greater than the cost of funds?"

Operations Management Operations managers use a huge tool kit of risk-balancing equations. One of the most basic equations is the "economic order quantity" (EOQ), which centers on stock-out risk. For example, if too much of a perishable product is ordered, it expires and is wasted. If too little is ordered, sales opportunities are lost. To calculate the EOQ given risk, this formula includes factors such as delivery time, cost of capital, and cost of storage space. Bar code check-outs have become important because they provide more precise data to calculate EOQ to manage stock-out risk.

> Internal auditors can help cross-pollinate risk methods across the organization.

Marketing Execution and Sales Management "What will be the year, quarter, month, week, and day-end sales?" This is the critical question from marketing and sales managers. Forecasting is vital to allocating marketing and sales resources as well as ordering the right quantities of the right products for the right locations. A key risk management method is analysis of the marketing-sales funnel. In the new world of online sales, "clicks" funnel stages include people aware of a product, aware of a seller, visiting a website, clicking around, putting a product in a shopping cart, ordering, ordering again, and telling their friends. Today's forecasts are cascades of probabilistic equations tracking the clicks through online shopping chains.

Human Resources Hiring and resource planning, from the initial job posting to the interview and selection process, is about risk management. What's the risk a job candidate won't perform as expected? Reducing this risk is the reason organizations engage expensive consultants to conduct personality surveys, emphasize employee benefits and retirement plans, and create on-boarding plans.

Quality Management Quality and risk are closely related. Quality is about the probability that products will meet expectations. Risk is about the probability of a defective product.

The Common Thread

For all their differences, these business disciplines share many risk-related concepts and assumptions. A common thread running through their risk management processes relates to the use of mathematical concepts, which have been refined over many decades. For all of them, math based on probabilities is central to managing risk. Other common ground includes:

- Managing risk is needed to enable taking risk—sometimes huge risk—to achieve objectives.
- Risk resides in a dynamic world of change, complexity, and fatigue. These are the three catalysts of risk.
- Each process requires an appreciation of systems, interconnectedness, and the need to understand deep root causes and process interactions.
- Asking "what if?" with scenario analysis is the heart of managing risk.
- Decisions seek to optimize risk and return.
- The roots of risk management are millennia old.

In short, appropriate risk mathematical and management methods matter. Internal auditors, while rotating their focus from one part of the organization to another, can observe and learn from each role's math and methods.

Cross-pollinating Risk

By learning from the risk methods in each business area, internal auditors can help cross-pollinate risk methods across the organization. Opportunities to cross-pollinate include bridging strategy and finance through the options modeling approach, smoothing the flow of risk math from all business areas into the risk calculation used inside options models or NPV, streaming together the quality improvement and sales risk analyses to make it more likely that quality will be free of cost, and encouraging teams to come together in scenario analysis workshops to more easily achieve shared business objectives. Each bridge built could become financial value created and personal trust earned. Ia

BRIAN BARNIER *is principal at ValueBridge Advisors in Norwalk, Conn. and Burnt Oak Capital in London.*

Fraud Findings

BY JENELL WEST EDITED BY BRYANT RICHARDS

LIFE OF LUXURY

A subsidiary president takes advantage of minimal oversight to embezzle more than US$2 million.

Candace Smith is a member of the internal audit staff at Ace Ltd., a large, diversified company with subsidiaries in numerous industries. While reviewing prior audit plans, Smith realized that one subsidiary, CRL Ltd., had not been subject to an internal audit since its acquisition five years before. When Smith was reviewing the financial results for CRL, she noted that actual expenditures were much higher than budgeted and historic figures. She met with the chief audit executive (CAE) and recommended that this subsidiary be included in the current-year audit plan. The CAE agreed with her assessment, and auditors began to look into CRL's history.

CRL was founded by Wayne Boyd when he was in his early 30s. Boyd had a larger-than-life personality and earned a reputation for lavishly entertaining customers and prospects. Seven years after founding CRL, he sold a majority interest to Ace for more than US$30 million. He remained president of the division, received a generous salary, and was given a US$500,000 annual stipend to cover his entertaining expenses at his various properties. He also had access to a corporate credit card and made frequent use of his expense account.

Accounting and other core business processes remained under Boyd's control and were performed by CRL personnel. Boyd was used to having total control over all aspects of CRL, which allowed him to play fast and loose with the accounting records. He regularly pushed his personal expenses through the company. When Ace took over, it implemented a budget, but day-to-day operations remained in the control of Boyd and his family.

When the internal auditors arrived, they identified many over-budget accounts and requested supporting documentation. Many of the supporting documents did not appear to relate to either CRL or Ace, but to Boyd's personal purchases. Internal audit began to interview CRL employees who were hesitant to speak with Ace representatives. While CRL's accounting personnel were not forthcoming, Boyd's personnel assistant, Mary White, was a wealth of information. She told Smith and the other internal auditors about Boyd and his personal financial habits.

After the acquisition, Boyd went on a spending spree, buying a plane, hunting lodges throughout the region, and a custom vehicle made for his daughter as a birthday present. Because CRL was located 750 miles away and its accounting staff was segregated from the rest of Ace, management at Ace was unaware of these extravagant purchases.

Boyd had numerous groundskeepers and

SEND FRAUD FINDINGS ARTICLE IDEAS to Bryant Richards at bryant_richards@yahoo.com

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

housekeepers who worked at his personal properties on CRL's payroll. Over the course of two years, CRL paid its staff US$610,000. Boyd also charged a variety of additional personal property expenses to CRL for fish to fill his private lake, a grill for cooking for clients, and a taxidermist for stuffing animals killed on hunting trips with customers.

In addition to his wife and children, Boyd also had a girlfriend. She received an annual salary from CRL of US$175,000, though she didn't actually work for the company. In his attempts to conceal the relationship from his wife, Boyd used his corporate credit card to pay for their meals and travel. When his wife became wise to these tricks, Boyd began to use his assistant's credit card.

Boyd also used some of the proceeds from his windfall to flip condominiums. He jointly owned some of these properties with a CRL employee who wrote a check to Boyd every month for his portion of the mortgage. As Boyd became desperate for cash, he stopped remitting those checks to the mortgage company and pocketed the money. The employee's credit score declined dramatically. Later, Boyd refused to pay any portion of the outstanding mortgage. Instead, he arranged to have the employee's pay increased to provide additional funds to pay it.

When Boyd purchased the plane and hired a pilot who didn't know how to fly, he had CRL pay for the pilot's salary and training. He prepared invoices and billed CRL for all of the flights, including those that were personal in nature. Fictitious invoices were submitted for flights that never occurred and wages that were already being paid by CRL to generate additional cash flow for Boyd.

Within five years, Boyd spent almost all of the money that he received in the majority sale of his business, but he continued to live a lavish lifestyle. When a collection agency started calling his office and he was desperate for cash, he began to use his business credit card and his assistant's to cover even more personal expenses. Boyd also would submit duplicate reimbursement requests through an expense report, despite the fact that they were already on his corporate credit card. In an attempt to conceal his fraud, Boyd damaged his receipts to remove the credit card number listed on the bottom. In just two years, he charged more than US$700,000 of personal expenses on CRL's credit cards.

Thanks to the internal audit team, Ace realized that it had a major problem with Boyd and CRL. Ace sent one of its executives to CRL's headquarters to get things in order. When the forensic accounting team was done evaluating the records, it appeared that Boyd embezzled more than US$2.2 million from CRL. He was terminated from the company but no charges were filed.

Lessons Learned

- When designing the internal audit plan, it is important to ensure that riskier business units receive adequate attention. In CRL's case, there were many red flags that should have drawn the internal audit team's attention sooner, including its geographic distance from Ace, the recent acquisition, and the fact that many key processes remained in the hands of CRL and its former management.
- When performing their work, internal auditors should consider interviewing employees and asking questions about their company's anonymous reporting hotline. Do employees know about the hotline and do they feel comfortable using it? Many employees at CRL knew about Boyd's fraud, but were unwilling to tell Ace until Boyd was terminated.
- Internal audit should consider performing random checks between personnel files and payroll records. All employees receiving a paycheck should have a personnel file. It is also important to perform periodic audits to ensure that all employees are receiving the appropriate rates of pay. Internal audit should determine if policies exist that govern who is allowed to adjust compensation and if those policies are being followed.
- Consider distributing paper paychecks (rather than direct deposit) randomly. This practice would have helped Ace identify ghost employees such as the girlfriend, pilot, housekeepers, and groundskeepers.
- Internal audit should determine if employees with corporate credit cards are also permitted to submit expense reports. If so, it may be beneficial to test some credit card purchases to determine if they are also inappropriately included on expense reports.
- Internal audit should review the acceptable use policy for all corporate-issued credit cards. This policy should clearly state the consequences for misuse of the card. Internal audit also should consider who was involved in designing this agreement—was legal counsel involved to ensure it is enforceable? If no such policy exists, internal audit should consider making a recommendation to management about its adoption and design.
- When reviewing existing processes and procedures, internal audit should determine if the accounts payable staff has had adequate training to spot questionable invoices. Internal audit should also evaluate the processes for resolving unusual items. Ia

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

AUDITOR SPOTLIGHT

CaseWare Analytics recently met Erin Baker, Data Analytics Program Manager for the University of Texas System Audit Office, and discussed her thoughts on data analytics. Here are some highlights from our conversation.

Q: How much of a role does data analytics play in your position at the System?

A: First, in terms of structure, the UT System consists of eight academic and six health institutions, as well as a System Administration component. For this reason, the data analytics activities that my team and I undertake are quite large and extremely varied!

Our activities include everything from assisting other audit departments on how to use data analytics in upcoming audits, to performing data analysis in specific areas of a project and then delivering those results for further investigation. We also develop customized analysis tools and scripts, and act as consultants by providing guidance on how other teams can grow their use of data analytics.

Q: What do you most enjoy about teaching others how to use data analytics software?

A: I find it satisfying to see my students get excited about IDEA's capabilities and how it can benefit them. Recently I trained a department that was struggling to compare two data sets with more than 300 different numeric fields from two different years. Their electronic reports indicated that there was an anomaly, but the description of the issue was extremely generic and diagnosing the source of the problem was complicated and time consuming.

With just a few clicks in IDEA, we were able to quickly identify all the anomalies and reduce the time needed to complete the project from days to hours—or even minutes. It was the coolest thing to watch as the auditors I was training began to realize the impact that IDEA could have on this and other projects!

Q: What advice do you give to anyone who is considering a data analytics tool?

A: Have realistic expectations! Even though IDEA is very easy to use, you have to take the time to learn how to use the software. You also have to understand the meaning of your data and be able to look at it in different ways. You rarely receive your data in a format that works for you, so be prepared to convert the data into a more usable format.

Start with some simple analysis to get a few 'easy wins' and learn about the tool's capabilities. But don't limit yourself! As you get more comfortable with the software, you will discover many things about what the data is saying to you.

To learn more about how IDEA can improve your audits, visit us at www.casewareanalytics.com.

CaseWare Analytics

Resilience through crisis

J. Michael Jacka

Illustrations by Gary Hovland

On April 20, 2010, an explosion at the Deepwater Horizon drilling rig started what is commonly referred to as the BP oil spill. Eleven people died and from four to five billion barrels of oil leaked into the Gulf of Mexico. During the ensuing public relations nightmare, BP took several questionable actions in terms of its accountability, acknowledgment of the accident's seriousness, and release of information to the public. The organization's negative perception was reinforced by CEO Tony Hayward's famous comment "You know, I'd like my life back." Over the course of this industrial disaster, BP suffered considerable reputational, legal, and financial damage.

Virtually every organization, regardless of size, geography, or industry, will face a crisis at some point. The chances are it will not be as significant as that faced by BP. But it's not a matter of if a crisis will occur, but when — and to what extent it will impact the business. The ability to recover — the resiliency to rebound from financial and reputational fallout — depends on steps taken well ahead of time to manage the event and, most importantly, the associated communications.

Internal audit can play an essential role in crisis preparedness. With the risks inherent in crisis management, an audit of the process may be a given. But internal audit can also provide

The ability to weather difficult times is crucial to the success — and even survival — of organizations.

invaluable assistance by remaining proactively involved throughout the development and implementation of any crisis management plans, and by participating in post-crisis analysis.

CRISIS TEAM

The key to an organization's ability to recover from the impact of a crisis is preparation. To ensure the organization is prepared, a crisis team should be established with responsibility for identifying potential crises, developing crisis plans, and educating and training all employees on how the plan will work.

As with any group responsible for identifying potential risks and related actions, the team will require individuals with the skill to methodically work through potential issues and resolutions. However, because the team will be actively involved during crisis management, members should also be fast thinkers who can make quick, real-time decisions.

The crisis team should be cross-functional, with representation from each major organizational division. Because crisis management is about communication, the organization's public relations group—whether in house or outsourced—will play an important role, as will the group responsible for brand management (usually the marketing department). And, while the team does not need to include the full executive management suite, it should have at least some executive-level representation. The team should also include representation from areas such as legal and compliance, to ensure regulatory and legal issues are considered.

Internal audit should also be part of the team. Although the auditors will have to ensure they are not directly involved in decision-making, which could negatively impact their independence, they can provide input to help ensure the team is addressing the appropriate issues.

CRISIS IDENTIFICATION

The team's first responsibility is identifying potential crises. To understand the circumstances that might lead to a crisis, team members should conduct a thorough review of external and internal influences that includes interviews with employees and other stakeholders. Based on its analysis, the team can develop a set of scenarios to serve as the foundation for crisis planning.

This is an area where internal audit's expertise can be invaluable. Auditors can provide insights from prior audits and work completed in enterprise risk assessments. Moreover, internal audit's interviewing and process analysis skills can play an important role in crisis identification and evaluation.

> **No crisis plan would be complete without specifically addressing communication protocols.**

The crisis team should also identify operational and communication issues that might cause or contribute to a crisis. It can then provide recommendations for systems revisions that could impact the potential for a crisis before it occurs.

In evaluating crises, the team should be prepared for situations where the organization has not caused a crisis but is part of an industry or territory where a crisis is occurring. For example, within a week of the U.S. Environmental Protection Agency announcing that Volkswagen had bypassed emissions control testing, Ford Motor Co. President of the Americas Joe Hinrichs announced, "We don't use defeat devices and we clearly understand what it means from an integrity standpoint to make sure our vehicles perform on the road like they do in the lab." Being prepared to separate your organization from such events can be just as important as preparing for its own crises.

CRISIS PLAN

Once potential crises are identified, the team should develop a comprehensive plan that provides a formal cadence for the organization's response. The plan should define each person's roles and responsibilities, as well as the specific processes and procedures to be followed for each type of crisis. At the same time, it should be designed to allow for the flexibility necessary to respond to constantly changing situations.

The crisis plan should include activation protocols: the events or situations that cause the crisis plan to be put in place. It should also provide a method whereby all employees can report potential crisis situations. Because front-line employees are often best positioned to see the early indicators of a crisis situation, providing them a reporting method gives the organization a better chance of getting in front of the situation—acting rather than reacting.

COMMUNICATION PROTOCOLS

Effective communication is fundamental to successful crisis management. In fact, some organizations refer to the crisis plan as the crisis communication plan. No plan would be complete, therefore, without specifically addressing communication protocols.

Stakeholders Rapid contact with all stakeholders—including employees, Fewer than **half** of board members say their organization has the **capabilities** or processes to handle a crisis with the best possible outcome, according to Deloitte's recent Crisis of Confidence survey.

THE PRISM OF PUBLIC PERCEPTION

One area often overlooked in discussions about crisis management is the impact of internal decisions on the public's perception of the organization. In particular, spending that is perceived by the public to be "lavish" can be the cause of serious backlash.

Any significant operational decision has a public relations component and should be considered in that light. Financial decisions that seem to make perfect sense in the boardroom may raise questions about the board's ability to carry out its fiduciary responsibilities, eroding investor, donor, or taxpayer support. For corporations, the bar for outrage can be very high. But nonprofits and governmental agencies have a smaller margin for error and need to maintain constant vigilance.

For example, in January 2016, CBS News reported on questionable spending by the Wounded Warriors Project, including increased expenses for conferences, travel, and public relations. A compelling argument could be made that only part of the organization's story was told. Nonetheless, donations to the veterans' charity decreased significantly after the report, and both the CEO and chief operating officer were dismissed. Whether the public's perception was correct or not, the incident underscores how internal decisions can be spread to the public in a way that paints the organization in a bad light.

Strategic and tactical decision-making represents an area where internal audit can have a positive influence. When conducting a review of any area, auditors can step back and view key decisions through the public's eyes. If they see the potential for anyone outside the organization to raise questions, practitioners should bring it to the attention of management and determine if any action is necessary. Moreover, the chief audit executive should keep this topic front and center in discussions with the board and audit committee.

customers, vendors, and volunteers—is essential. The plan should include details on the notification systems used for initial contact, as well as ongoing updates. And while call trees are a fundamental part of any notification system, the organization must be prepared to use multiple modalities—emails, texts, social media, etc. To ensure timely and complete communication, a comprehensive list of stakeholders' contact information must be maintained and constantly updated.

Perhaps most importantly, the plan should describe how notifications and feedback will be coordinated with executives and the board. Details should include the format for reporting, the information to be included (e.g., customer impact, financial impact, and media coverage), and expectations of how often (usually daily) and when updates will be received. Careful planning helps limit the barrage of phone calls from executives seeking the latest information.

Spokesperson The single most important aspect of crisis communication may be the organization's official spokesperson. The crisis plan should identify who will act in this role, as well as a list of backup spokespersons who may be called on depending on the situation, the location, and the availability of personnel. For example, if an immediate response is needed at a location before the official spokesperson has arrived, a backup should already be identified. The plan should also outline restrictions placed on anyone else who might be contacted for information.

The spokesperson must possess the right skills and hold an appropriate position within the organization. Often, the responsibility falls to the organization's highest level of authority. But if that individual lacks the necessary communication skills, someone else at the executive level should take on the role. Many experts agree that BP's Hayward was a poor fit as the organization's spokesperson, and that any turnaround in the dialogue with the public was the result of Executive Director Bob Dudley taking on the role.

Anyone who may be called upon to serve as spokesperson should receive in-depth training. Generally, training in media interview skills is not a focus for executive managers. And just because someone can speak to a crowd effectively does not mean he or she is prepared for the media onslaught a crisis can elicit. Training should come from professional services, and it should be reinforced regularly—to the point where the individual falls into the spokesperson role without a moment's hesitation.

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

Media The crisis plan's media-related protocols should be twofold. First, they should include guidance on crisis response messages. Although complete statements cannot be developed up front, the organization should design general messages tailored to the scenarios developed by the crisis team that can then be adapted after a crisis breaks.

Crisis communicators should immediately engage the media through open and honest communication.

Second, the plan should include detailed information regarding members of the media who will be involved in communications, including television, radio, print, and social media. Rather than viewing the media as a liability, crisis communicators should immediately engage the media through open and honest communication, using them as a resource in managing the crisis. If possible, the organization should reach out to the media before the media contacts the organization.

Moreover, the organization should establish effective working relationships with the media well before a crisis occurs. Strong relationships will help give crisis communications a firmer footing and allow the organization to identify individuals who may be counted on to give a favorable, or at the very least balanced, reporting of events.

VALIDATION AND UPDATES

Internal audit should provide validation throughout the development and update phases, providing assurance that a crisis assessment has taken place, a comprehensive crisis plan has been developed, training and practice activities have been implemented, and alignment with the initial assessment has been achieved. While the organization may have in-house crisis management expertise, external experts should also be brought in to provide additional knowledge and an objective analysis of the plan. Validations—internal or external—should be repeated every few years, or whenever significant events warrant a new review.

The crisis team must constantly update its analysis and adjust the plan as necessary, and it should establish a system that enables stakeholders to provide input on potential issues. To facilitate updates, the team should meet monthly, or at least quarterly, to ensure emerging events are considered and the plan reflects the most current conditions.

TRAINING AND PRACTICE

A crisis plan is useless unless people understand when and how it should be implemented. All employees should receive training to understand their roles and be able to implement the plan flawlessly.

The organization should also conduct crisis simulations. A set of scenarios representing the broad range of potential crises should be developed, Just over 50% of senior executives say their organization takes steps to monitor for reputational risk issues, according to Standing Partnership's 2016 Reputational Risk Report.

TONE OF COMMUNICATIONS

People do not remember the specifics of a crisis as much as they remember the organization's response. Accordingly, the success or failure of crisis management often hinges largely on communication.

In most cases, successful crisis communication starts by saying "I'm sorry," and saying it with candor, sincerity, compassion, sympathy, and even embarrassment. This is, in part, why the spokesperson's training is so important—without understanding how best to deliver the message, it can far too easily ring false.

The response to the crisis must be prompt—a public acknowledgement of what has occurred—or rumor and innuendo will fill the gap. Communication must be honest (no spin) and provide as much explanation as is available. It should answer the basic reporter questions—who, what, why, when, where, and how—sharing as much about the error or oversight as is known. If nothing is known, then this should be admitted.

The organization should publicly commit to taking specific, positive steps to address the issue and emphasize its commitment to doing what is right. The actions that follow must support those statements, without any signs of waffling. As those actions are taken, the organization should communicate what has been accomplished, what is left to achieve, and how it will be done.

This approach may not be popular with some, particularly many legal experts, but crisis management experts contend it is the best way to manage negative events. And it is the best way to bring the company back from its reputation nightmare.

and personnel should be run through the full gamut of these experiences. This exercise will prepare employees to act quickly, decisively, and accurately, while maintaining the flexibility necessary during an actual crisis. The simulations also provide an opportunity to identify plan improvements before a crisis occurs.

Internal audit should take a role as observer in all simulations. It should provide assurance the plan is working as designed, and, when activated, is providing complete coverage for all potential issues.

THE CRISIS OCCURS

If a comprehensive crisis plan has been developed, tested, and fully integrated within the organization, members of the organization should be able to execute it with little hesitation. The effects of the crisis, while still impactful, should be greatly reduced, helping ensure the organization's resilience in recovering from the reputational onslaught.

During the crisis, beyond any role that may be defined in the crisis plan or as a part of post-crisis evaluation, internal audit will want to serve as an active observer and help ensure the plan is executed as designed. Plan implementation includes flexibility, and internal auditors can provide instant feedback to help the crisis management team see where such flexibility may be necessary. The auditors can also serve as outside observers, advising on bigger picture issues that may be overlooked as the plan is carried out.

AFTER THE CRISIS

Once the crisis is over, the organization should evaluate the plan's performance. Without a thorough post-crisis analysis, preparedness and response are unlikely to ever improve. Internal audit should be included in any self-assessment efforts conducted by the organization; outside experts may be of benefit as well.

The types of questions that should be asked in any self-assessment include:

- Were there signs that could have provided an earlier warning that might have helped forestall the crisis?
- What were the weaknesses and vulnerable points that allowed the crisis to occur?
- How effective were internal and external communications?
- Were the right people on the crisis team? Who excelled and who failed?
- Is additional training required to bolster effectiveness?
- What was done well and what could have been done better?

All levels of management should receive the results of these postmortems. The board, in particular the audit committee, should also be involved, ensuring any necessary corrective action is taken.

ROAD TO RECOVERY

For an organization to have the resilience to bounce back from a crisis, it must be prepared. And as a key steward of organizational well-being, internal audit can maintain both active and proactive roles. Being involved in crisis analysis, plan development, training, and plan execution, internal audit can help ensure the organization does crisis management right. And in the process, it can help make organizational resiliency a part of all operations. Ia

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

Hit the Ground *Running*

With internal audit filling many of its open positions from intern pools, a well-designed internship program is a must.

Dennis Applegate
Sarah Bee
Dominique Vincenti

College interns have become a key source of new employee hiring in Fortune 500 companies, according to Jeffery Selingo, author of *There Is Life After College.* Data from the Collegiate Employment Research Institute at Michigan State University presents compelling evidence supporting Selingo's claim. Based on the Institute's 2015-16 Recruiting Trends, companies with more than 10,000 employees now convert about half of their interns to full-time employees.

The trend in hiring interns and retaining them as full-time employees has impacted many major internal audit departments. Nestlé Purina not only advertises its internship program, but empowers its interns to join the company full-time immediately upon graduation. Interns travel up to 50 percent of the time auditing Nestlé business units in Canada, Mexico, and the U.S., working within operational audit teams of the Nestle Market Audit group. Through this experience, interns "accrue a deep knowledge of the business very quickly," the company reports. As such, interns are viewed as a rich source of new audit talent.

"Internships have changed the dynamic of recruiting on a national scale," says Jon Gonzalez, a recruitment partner for Deloitte. "Most CPA firms are making their intern hiring decisions much earlier in the process to compete for top talent."

Because employers are increasingly hiring from their intern pools rather than through traditional college campus recruitment, many college career service organizations have had to change their on-campus internship recruiting schedules to stay in sync with recruiting practices. For example, the University of Pennsylvania's

“Based on the needs of the department, we may offer qualified interns the opportunity to transition to part-time positions.”

Jeff Davis

“As a relatively small department of 26 staff members, I have to set high expectations for interns.”

Scott Howe

Career Services moved its internship recruiting from February 2017 to October 2016 to stay in sync with employer recruiting practices.

TRADITIONAL STAFFING SOURCES

Historically, many companies filled their vacant internal audit positions from within the company, selecting employees with broad financial or operational knowledge or with solid management experience. Looking inward to fill open positions stems, in part, from the idea that internal auditors must have experience in the complexities of a company and its processes and procedures to successfully accomplish professional audit work. Indeed, some chief audit executives (CAEs) have recruited existing managers from within their organizations not only for those reasons, but also for their ability to connect, given their background, with client management.

However, in recent years, internships have increasingly become an important source of internal audit hiring given the technical training that interns receive and the performance capability that they have already demonstrated. Equally as important, skilled interns learn how to interact professionally with the company workforce and client management during their internships. These soft skills vary depending on the industry and corporate culture. But such skills give certain interns a performance advantage, if hired, because they already know the corporate behavior expected. Because of the reduction in hiring risk, the strategy of some firms is to always select internal audit interns with the goal of offering them full-time employment.

CAE SUPPORT

CAEs rarely hesitate to hire an intern whose work performance comports with expectations. Robert Thieling, former executive director of Audit Services at Group Health Cooperative, a large health maintenance organization covering the Pacific Northwest, and new vice president of internal audit for MedImpact Healthcare Systems in San Diego, began an internship program immediately upon assuming his CAE responsibilities at Group Health 11 years ago. “There was not an intern we wouldn’t have hired full-time,” he says. “Some we lost to CPA firms doing internal audit consulting, but that only proved the value of the program and the quality of our interns.”

Similarly, Expedia has leveraged its internship programs to supplement the company’s internal audit team during peak periods, viewing internships as a less costly staffing alternative. Jeff Davis, Expedia’s vice president of Corporate Audit Services, is using the company’s human resources (HR) department to standardize intern hiring and leverage the other HR disciplines to actualize even more of the internship program’s cost-saving benefits. The number of audit interns at Expedia has averaged two to three per year, according to Davis. “Based on the needs of the department, we may offer qualified interns the opportunity to transition to part-time positions for further professional development.”

Scott Howe, vice president and CAE at Costco, also relies on a corporatewide internship program for most intern staffing, though he will hire directly if a prospective intern reaches out to him with a special interest in internal auditing. Since becoming CAE for Costco nine years ago, Howe has hired several interns into permanent positions.

“If positions had been available, I would have hired more. Overall, one out of every two interns meets my expectations,” Howe says, a figure consistent with the industrywide conversion rate of interns to full-time employees. “As a relatively small

35% of respondents plan to increase their intern hiring targets in 2017, according to Recruiting Trends 2016-2017 from the Collegiate Employment Research Institute.

department of 26 staff members, I have to set high expectations for interns."

These and other CAEs see internship programs as providing great opportunities for early-career employees to observe many company functions and locations, leading to a thoughtful consideration of different career paths.

INVESTMENT IN INTERNS

Some internal audit departments may lack the management breadth to support another professional development program. Some CAEs have noted that upwards of one-third of their internal audit staff members are rotational in nature, participating in companywide professional development programs supported by internal audit. While such programs have tremendous potential for developing future corporate leaders, they can also strain the department's infrastructure. To be successful, an internship program requires a significant investment of time.

Brooke Vatheuer, CAE for Alaska Air Group, has taken the planning and organizing of her internship program to a whole new level. "By the time the internship commences, we have planned out their activities for a 12-week period—everything from facility tours to audit assignments to happy hours with other interns and leaders," Vatheuer says. "We recognize that an intern's primary job is to learn, so we build plenty of coaching and development time into their schedule."

One note of caution: Training and indoctrinating internal audit interns may entail substantial cost given their potential lack of professional business experience. Moreover, closer supervision of interns is often necessary to ensure continuity of audit work product quality. Nonethess, many firms have determined that the benefits derived from identifying and hiring talent from their intern pools offset the added indoctrination training and supervision cost, justifying their investment in an internship program.

REAL-WORLD INTERNSHIPS

Goldman Sachs Internal Audit interns shadow and assist audit teams, attend seminars and presentations, and participate in networking events. This experience is designed to provide the intern "with a real sense of what you would be doing day-to-day as a full-time employee," according to the description published in the firm's intern job announcement, indicative of the rationale for such an investment.

Lithia Motors, which broke into the Fortune 500 at No. 482 in 2015, not only encourages, but prefers, that its internal audit interns join the company as full-time auditors upon graduation, which is stated as an explicit goal of Lithia's internal audit department on the company's website.

At retailer Nordstrom, all of the interns working on compliance with the U.S. Sarbanes-Oxley Act of 2002 have landed full-time positions at Nordstrom, a major CPA firm, or another Fortune 500 company. Moreover, half of all Nordstrom interns are hired into the company, including internal audit—a figure consistent with Collegiate Employment Research Institute data.

BEST PRACTICES

Many of the CAEs interviewed for this article have taken a traditional approach to managing their intern programs—planning, organizing, controlling, and directing them to a successful outcome. The following key attributes of a well-designed internal audit intern program, including selected outcomes or processes for each management function, originate from a working group of internal audit management professionals who serve on Seattle University's Internal Audit Advisory Board. Companies such as Amazon, Boeing, Expedia, and Nordstrom are represented on the board, along with Deloitte, PricewaterhouseCoopers, and EY.

Planning—preparing job descriptions, program budgets, and a hiring plan and schedule.

What the intern will do and is expected to accomplish is explained in the job description. Many firms state the goal of their intern program in the

TO COMMENT on this article, EMAIL the authors at dennis.applegate@theiia.org

"We recognize that an intern's primary job is to learn, so we build plenty of coaching and development into their schedule."

Brooke Vatheuer

"Some [interns] we lost to CPA firms doing internal audit consulting – but that only proved the value of the program and the quality of our interns."

Robert Thieling

description, such as identifying future internal auditors or augmenting existing staff. In either case, it is important to emphasize not just the meaningful nature of the work experience, but the availability of mentors, career guidance, and specialized professional training, such as data analytics or certain program applications.

To capture the true financial impact of an intern program, most companies prepare an operating budget containing not just the direct costs, but also the indirect costs, including audit supervision and intern training. Predetermined start and end dates for the annual intern program drive the budget. Because it is discretionary, many companies will address it annually based on audit plans and hiring needs.

Working with internal audit management and hiring support organizations—such as HR, recruiting, and leadership and development—helps create a plan and schedule that include enhanced coordination and communication in the hiring process while mitigating the risk of selecting the wrong candidate.

Organizing—assigning audit management, appointing mentors, and orienting new interns.

The assigned audit manager must arrange intern work space, training, and building and system access, and remain available on site to give help or serve as a sounding board until the intern is integrated into the organization. To ensure adequate communication, weekly one-on-one meetings between manager and intern are a best practice. Most managers will routinely invite interns to all-team meetings and functions as soon as they are on board. Given the demands of intern management, most companies require the assigned manager to have substantial audit management experience before giving them internship oversight responsibility.

Mentors provide audit coaching and career guidance. Some companies appoint a mentor within the internal audit department to provide hands-on audit guidance and another mentor outside the department to guide and develop the intern professionally. Often, the latter mentor is at the senior management level.

A formal orientation normally defines company expectations for an internship; identifies internship program management (where to get help); overviews the company business and corporate functions; explains the internal audit organization and its policies/procedures; and emphasizes professional standards for timeliness, customer service, and due diligence. Most companies stress that interns must take responsibility for their own work performance and professional development, so they are encouraged to document their work activity and accomplishments and seek feedback from their immediate management and company mentors.

Controlling—establishing intern work objectives/schedules, performance feedback, and remedial action.

To ensure a positive work experience, audit management establishes intern objectives and sets professional expectations early on as a performance evaluation tool. Most firms permit work schedules to be negotiated during the school year provided that the requirements of the master audit schedule are met.

Periodic performance reviews typically are conducted based on mutually agreed-to performance criteria, including leadership, ethical, or behavioral principles adopted by the company. Specific feedback is rendered, incorporating the observations of relevant auditors, project managers, and audit client management where appropriate. Most firms summarize

Employers **begin recruiting** interns **8 months** before their start dates, according to the 2016 Interns and Co-ops Survey Report from the National Association of Colleges and Employers.

strengths and weaknesses of the intern being evaluated, and nearly all identify improvement opportunities.

Remedial action where needed is critical for professional growth. Improvement plans are normally developed consistent with company HR practices and with an eye toward enhancing intern performance as an eventual full-time auditor.

Directing—assigning intern training and audit projects and communicating and coordinating internship activities.

Intern training generally focuses on audit tools and techniques for data analytics, enterprise resource planning for audits of business functions, and audit sampling for testing a population. Linking the prescribed training to the initial audit assignment is considered a best practice, which prepares interns to hit the ground running.

Guidelines should be established before assigning audits to interns. Above all, the audit project must be interesting and challenging and provide some fun along the way. Key criteria to consider include the extent of exposure to a variety of company locations, processes, and systems, and whether the audit can be scoped to the intern's employment period while still allowing participation on other audit projects. While their assigned audits are certainly contained in the master audit plan, interns are rarely assigned a project ranked critical on the risk assessment heat map.

SKILLS IN DEMAND

Some internal audit departments remain resistant to internships because the educational system has not always taught the skills that internal auditing and similar professions demand. Many colleges and universities today recognize that deficiency and are preparing students for knowledge transfer to the workplace by combining education with relevant work experience. Some schools even offer college credit for internships.

As for internal auditing, some schools administer certificate and post-graduate programs specifically designed to teach students not just internal audit concepts and techniques, but how to apply them to actual audit projects. For example, students enrolled in Seattle University's internal audit program support campus administration by routinely auditing functions such as finance, facilities, HR, and IT as part of the internal audit curriculum. The master audit schedule and project findings are coordinated through the university's chief financial officer and presented to the audit committee of the board of trustees, giving students hands-on audit experience. CAEs willing to undertake the challenge of an internal audit internship program may be pleasantly surprised by students who are well-prepared for the professional challenge.

Based on lessons learned from her oversight of internships during the past several years, Mindi Work, vice president of finance for Symetra Financial, offers this advice: "Stretch them, give them real assignments, and let them be a little uncomfortable. They are not there to job shadow. It will truly be a valuable experience if they contribute meaningful work to the audit department." Ia

DENNIS APPLEGATE, CIA, CPA, CMA, CFE, *is a lecturer and adjunct professor of internal auditing and accounting at Seattle University.*

SARAH BEE, CIA, *is director of internal audit programs and a senior instructor at Seattle University.*

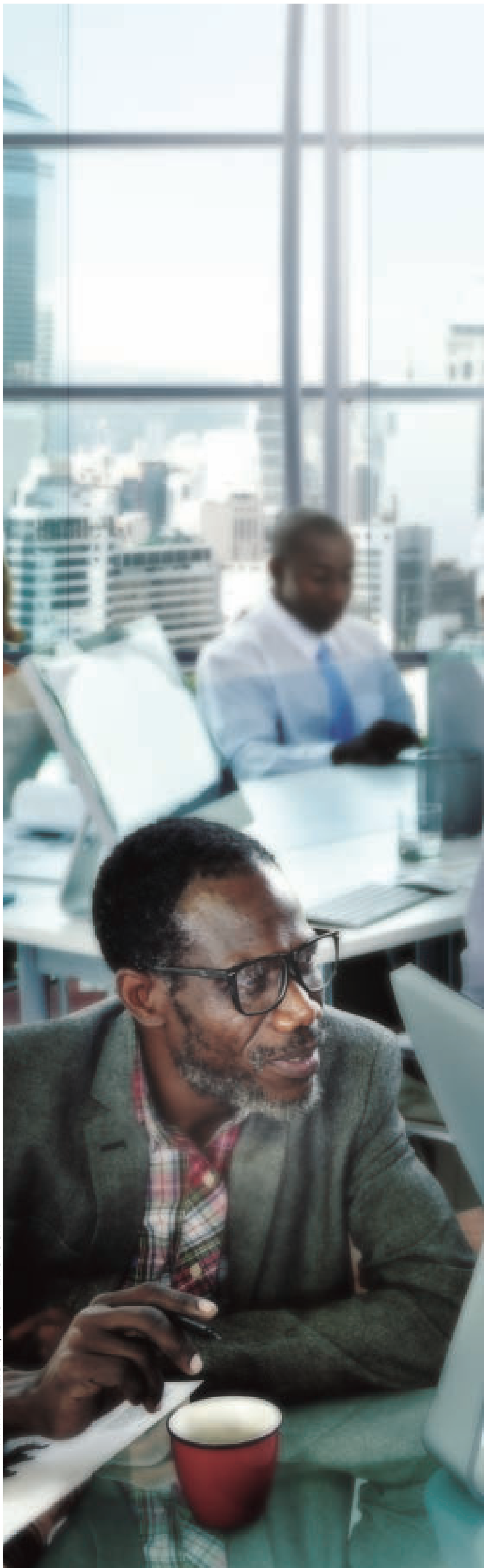
DOMINIQUE VINCENTI, CIA, CRMA, *is vice president, internal audit, at Nordstrom, and chair of the Seattle University Internal Audit Advisory Board.*

"Stretch them, give them real assignments, and let them be a little uncomfortable. They are not there to job shadow."

Mindi Work

Many internal audit departments are turning to maturity models to deliver opinions about organizational performance.

Jane Seago



RAWPIXEL.COM / SHUTTERSTOCK

Sometimes, a binary answer isn't enough. At least, that is the belief of the thousands of organizations that have used a maturity model to assess their progress in achieving certain goals since maturity model concepts were introduced in the 1970s. They have found the model's reliance on a scale—often 1 (initial) to 5 (optimized)—to assess their performance in specific areas a useful guide for accomplishing two important objectives: understanding where the organization stands currently and coming to agreement on where it should be.

Initially focused on the IT function within an organization, maturity models have expanded into many distinct disciplines, such as project management, quality management, business process management, learning, human resources, supply chain, sustainability, social media, and security assurance (see "Maturity Model Examples" on page 41). Regardless of their niche area, effectively configured models tend to encourage in-depth conversations among a range of stakeholders and enable nuanced and

Climbing the scale

"Maturity models can be a much more engaging experience for the audit client/management as compared to a pass/fail assessment or other opinions."

James Rose

"A maturity model provides the audit client a clear understanding of risk levels and which controls fit the situation to create a better control environment."

Carmen Ozores

goal-driven thinking about targeted areas. As such, they are a valuable tool for internal auditors who have come to realize, over time, the benefits of moving beyond a "black and white" approach to audit findings and the support that the range of levels provides in helping auditors discover the gaps between current and desired states. Once auditors have identified and quantified the gap, they can begin searching for the root causes that hinder achievement of the desired state and zero in on appropriate recommendations to bridge the gap.

"Maturity models can be a much more engaging experience for the audit client/management as compared to a pass/fail assessment or other opinions," says James Rose, chief financial officer of Aperture Credentialing in Louisville, Ky., and author of the IIA Practice Guide, "Selecting, Using, and Creating Maturity Models: A Tool for Assurance and Consulting Engagements."

Some of the "engaging experience" may arise from the availability of a broad spectrum of labels. Alyssa Martin, executive partner, Advisory Services, for Weaver in Dallas, notes that internal auditors often are confined to using black or white answers: compliant/noncompliant, effective/ineffective. In her view, maturity models are exactly the "right paradigm" to evaluate the effectiveness of management systems such as governance that require many judgment calls. That is because those who work regularly with judgment calls may be more comfortable with a more subtly defined range of evaluations, rather than a simple yes/no, right/wrong finding.

CHANGING THE CONVERSATION

Use of a maturity model changes the nature of the conversation about the audit. The levels of incremental maturity lend themselves to acknowledging the organization's advances to date, creating a positive, collaborative tone. Recognizing these successes creates a more receptive audience when internal auditors present the verbal and written reports outlining the path to improvement.

Before the full benefits of maturity models can be realized, the groundwork has to be laid via pre-audit planning discussions among internal auditors, process owners, and management. "The discussion defines the different levels of maturity and establishes up front with the client what the expectations are within the maturity spectrum," says Kayla Flanders, senior audit manager with Pella Corp. in Pella, Iowa. "It takes more effort before the audit, but it helps significantly throughout the audit and at the end of the engagement when discussing issues and the overall report rating based on that upfront alignment."

She offers this example, related to financial reporting. Confer with the audit client to decide what attributes fit into each maturity category — mature, baseline, etc., reflecting both where the client is and where the organization expects the client to be — and then test to those attributes. In the mature space, an audit client may be using data analytics to identify specific anomalies or gaps in a process to review. This more effectively manages the risk by identifying anomalies based on outlined criteria and reviewing, typically, all transactions. At the baseline level, the client may be reviewing only individual significant transactions over a specified dollar value. This clearly manages the risk at a different level. Controls typically build on one another, so the client may still be doing the baseline activity or, as it moves into the mature category, it may find a need to focus less on some of the lower-level controls or eliminate them altogether. If the client is not yet where the organization expects it to

Internal auditors should **determine** whether the maturity model was **selected** and applied based on adequate criteria, notes The IIA Practice Guide, "Selecting, Using, and Creating Maturity Models."

MATURITY MODEL EXAMPLES

There are nearly as many maturity models as there are business functions to be measured. Here are a few models that may be useful for internal auditors:

- Capability Maturity Model Integration (CMMI), from the CMMI Institute (available in formats tailored for development [CMMI-Dev], service establishment and management [CMMI-SC], and product and service acquisition [CMMI-ACQ]).
- Cybersecurity Capability Maturity Model (C2M2), from the U.S. Department of Energy (also available in formats tailored for the electricity [E-C2M2] and downstream natural gas [DNG-C2M2] subsectors).
- COBIT 4.0 and COBIT 4.1, from ISACA.
- Portfolio, Programme, and Project Management Maturity Model (P3M3), from Axelos.
- Risk Maturity Model (RMM), from The Risk Management Society.
- Test Maturity Model integration (TMMi), from TMMi Foundation.

be, the internal auditor can reflect in the report the existing level, the level expected by the organization, and the work the client is doing to get to the desired stage. The report also can clearly communicate what attributes are missing (typically already known by management) to move the client into the next defined level of maturity.

Communication is also high on the list of benefits for Carmen Ozores, internal audit manager at HUCAM-Ufes, Ebserh (Empresa Brasileira de Serviços Hospitalares) in Brazil. "The common language helps in communicating assessment results, which makes the information clearer to support decision-making," she says. "For example, a maturity model provides the audit client a clear understanding of risk levels and which controls fit the situation to create a better control environment."

Not only is a common language fostered by the use of maturity models, it is a language that tends to be less inflammatory than many binary options, such as "ineffective" and "unsatisfactory," and more focused on process than on people. It ensures, in a non-threatening way, that stakeholders understand precisely what internal auditors mean when they recommend actions to move from one level to the next.

ASSURANCE AND INSIGHT

The work internal auditors do with the client to develop an understanding of what the model contains and how it is used ultimately helps progress the audit and enables the auditors to leverage the efficiencies the model offers. Brian Selby, director, Internal Audit–IT, at Discover in Riverwoods, Ill., notes, "Good tools, such as maturity models, help staff be more productive in their endeavors and deliver a better-quality product and service by acting as a source of improvement ideas." For example, although an organization might be performing risk assessments, the auditor may find that new risks keep materializing and destroying value. "By looking at higher-level maturity model practices for risk management process areas, the auditor can identify dynamic risk assessment approaches as a way to increase the likelihood of identifying new risks more timely," he explains.

In that sense, leveraging maturity models aligns with the use of appropriate tools called for in the *International Standards for the Professional Practice of Internal Auditing*, specifically, Standard 2210.A3: Engagement Objectives:

"Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board."

For Martin, the benefits of using maturity models are even more straightforward. They help internal auditors perform two of their most critical functions: providing assurance and insight. "Assurance is advising the client that the area is achieving the expected level of maturity," she explains. "Insight is identifying the root of the differences between the current and the desired state and defining the barriers to achieving expected performance levels."

Using maturity models in this way may be particularly effective for business areas that have a documented, internationally recognized framework such as The Committee of Sponsoring Organizations of the Treadway Commission's updated *Internal Control–Integrated Framework*, ISACA's COBIT, and the International Organization for Standardization's ISO 27001 and 22301 standards, says Anthony Noble, vice president of IT audit at Viacom Inc. in New York. He explains, "Having the structure of an internationally recognized framework to assess against enables us to use the literature generally available to easily partition areas to review and then evaluate their maturity level."

USE CAUTION

Despite their benefits, maturity models are not always the right solution. Like any approach an internal auditor may take, use of maturity models needs to be thought through carefully to optimize the benefits and minimize downside aspects as they relate to the organization and the intended outcomes of the work.

One potential drawback to maturity models is the temptation they may provide auditors to push the organization to higher maturity levels of performance than it is willing or able to adopt. This situation requires internal auditors to be seasoned enough in their thinking to accept that not every aspect of the audit needs to be at the highest level of maturity. Each organization must determine, based on a risk assessment, the appropriate amount of investment to make in achieving a degree of maturity for a process or procedure. Although the automatic assumption may be that every process should be at the highest level of maturity (level 5), that may not be the case, depending on the organization's core business, environment, and risk tolerance. If the consensus is that a level 3 or 4, rather than a 5, is appropriate for the process, then being assessed at that level is not a failure. Indeed, the range of acceptable options is one of the strengths of using maturity models.

"If, per a risk-based assessment, a given activity is appropriate at a lower level of maturity, auditors ought not recommend additional resources be spent for the sole sake of advancing to the next level," notes Debbie Shelton, director, IT Security & Compliance with LG&E and KU Energy, in Louisville, Ky. "Rather, auditors should work to understand management's process for determining the risk involved, the appropriate level of maturity, and the matching of the two." Based on this understanding, auditors can determine whether the assessment assumptions are sound, decide whether management adhered to its processes, and consider whether recommending something additional is needed to help the client meet functional objectives.

A concern sometimes expressed about maturity models is their inherently subjective nature, which can manifest itself in inconsistency. That inconsistency, in turn, is likely to result in limited assurance of reliability regarding the assessor, the assessment's quality, and the usefulness of market benchmarking. The Capability Maturity Model Integration (CMMI) Institute has created a formal certification, the Standard CMMI Appraisal Model for Process Improvement program, to address the subjectivity/consistency issue.

Assessing compliance may be an area where maturity models should be used with caution, if at all. "The expectation today is that the organization is 100 percent compliant," Rose says. "However, practically speaking, there are always things that can be improved, including compliance." Therefore, if the organization's assessment reflects anything less than the top level of maturity in compliance, legal issues may arise if a major compliance issue occurs. This doesn't necessarily preclude use of a maturity model, but Rose suggests taking great care in defining the model's categories and wording so there is no inference of a lower degree of commitment to compliance on the organization's part.

Other areas that may not be entirely conducive to using maturity models include those that lack a widely published international standard for the function, Noble says, citing human resources, accounts payable, and accounts receivable as examples. "For areas such as accounts payable, there are many ways to perform the task at hand and no internationally recognized standards to measure the area against," he explains. "We can evaluate the capability maturity model level from 0 to 5, but it is harder to determine what additional processes would move the area from a level 3 to a 4, for example."

Ultimately, maturity models represent a judgment of sorts. So, despite efforts to get everyone on board during pre-audit discussions and the use of less inflammatory language, there is no guarantee that difficult conversations will not arise after the audit. Flanders recommends auditors keep in mind that with maturity models, as with other, more traditional rating systems, "there is still a bottom and a top end of the scale, and no one likes to be at the bottom."

TIPS FOR SUCCESS

As internal auditors increasingly adopt the use of maturity models, their experience with them grows and lessons are learned, making each new audit run more smoothly and effectively. Internal auditors who have experience with maturity models provide several tips to get the most out of them.

Choose Wisely Selby notes that not all of the published maturity models contain the rigor of the most commonly used and widely available models, citing as an example the CMMI-Dev v1.3 report, which dedicates 300-plus pages to defining in detail the model levels for the generic and process area goals and practices related solely to software development activities. Choosing a model that reflects the collective wisdom and experience of many professionals and practitioners and is subjected to peer review and testing can help increase the internal auditor's consistency and credibility.

Be Flexible It may be advisable to embrace more than one model, using

VISIT InternalAuditor.org for tips about how to select a maturity model.

"If metrics for the area are well-defined, you can make actionable recommendations for change."

Alyssa Martin

"For areas such as accounts payable, there are many ways to perform the task at hand and no internationally recognized standards to measure the area against."

Anthony Noble

different models for specific functions under review. Shelton suggests starting by determining whether a maturity model is already being used by management of the function under review. If so, determine whether the model is suitable; if it is, use it for the audit. In this way, the client already understands the model, and perhaps already has completed his or her own assessment. This gives the internal auditor more time to review the evidence of maturity and recommend next steps, if needed, within the given risk profile.

Build the Best Model Ozores is a strong proponent of building a customized model, using an understanding of the audit client's environment to tailor standard frameworks. She suggests adding examples or making fine adjustments to the published model's language, so the result accurately reflects the environment under review. She counsels, "Depending on the field, there can be slight differences in language that make a great difference in final understanding."

Find a Champion In some of his previous organizations, Rose reports that the internal audit departments designated a methodology champion. That individual reviewed reports from a consistency standpoint, trained staff, and maintained the policies and procedures of the department. Given the rotation of audit team members, the champion improved consistency, thus mitigating risk and ensuring a quality assessment.

Mind the Gap Noble suggests baselining the maturity of various IT areas against desired maturity levels to build a useful gap analysis identifying improvement opportunities. He and his team use the published control framework literature when possible to provide a list of needed procedures for each area's level of maturity to facilitate identifying the gaps. He further suggests creating a graphic representation of the maturity model gap analysis, which he considers useful to aid senior management in understanding how close it is to achieving the desired maturity in several areas at once.

Be Prepared for High Ratings An area's maturity level is not always lower than its target state. In some cases, the area may be performing at a higher level of maturity than that agreed on in the planning discussions. This represents an opportunity to reallocate resources. Martin suggests, "If metrics for the area are well-defined, you can make actionable recommendations for change."

BEYOND BLACK AND WHITE ASSESSMENTS

When the appropriate maturity model is selected, tailored, or built from scratch, and agreed on in advance with the process owners and management, its use can enable internal auditors to provide nuanced indications of maturity levels. If a level is lower than expected, the auditors can uncover the root causes barring the path from the current state to the desired state and offer recommendations for continued improvement.

And these functions can be communicated using language that enables internal auditors to avoid the traditional perception of being critical or judgmental, seeing only black and white. Flanders notes, "Think about how we talk about ourselves. We assess internal audit departments as to their level of maturity using terms like 'assurance provider,' 'problem solver,' and 'insight generator.' We certainly don't call ourselves 'ineffective.' Why wouldn't we use a similar process for our clients?" Ia

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

From the Same Playbook

Arthur Piper

Illustration by Sandra Dionisi

By aligning its work with the organization's strategy, internal audit can help assure that the business is on the right track.

Predicting the biggest potential risks businesses face has become something of an industry. Consultancies, think tanks, and others produce surveys, reports, and ranked listings of what they consider to be the greatest threats to the success of governmental and corporate strategies. In 2017, geopolitical risk featured heavily, as did the threat from environmental disaster, terrorism, disruptive technologies, and demographic change—see, for example, the highly respected Global Risks Report 2017 published by the World Economic Forum.

But do these tectonic shifts of the global risk landscape, which threaten to derail an organization's strategic objectives, ever make it onto a chief audit executive's (CAE's) annual audit plan? And should they? Does the magnitude of the new challenges mean that the role of internal audit needs to evolve to address them? Opinions are split about internal audit's role in providing assurance around the risks affecting company strategy. Some boards want internal audit involved, some do not. Some internal auditors want to contribute to strategic assurance, others are led to prioritize compliance-related auditing.

"There is a sense today that in an innovative, disruptive, and fast-paced environment, someone needs to start providing assurance around risks affecting company strategy," Paul

Walker, the Zurich Chair in Enterprise Risk Management at St. John's University in New York, says. "If the CAE is willing to step up and demonstrate that he or she can add value, that's a win for everybody."

Walker says some CAEs are well placed to execute this role. "Some CAEs I've met are brilliant people with amazing business acumen, and the executives and the board in their organizations want them involved," Walker says. "They recognize the value of having that person involved and may not even see them as an audit executive—but instead as a trusted business advisor."

AN AUDIT DISCONNECT

It is unclear how many auditors are already fulfilling this role. In 2015, The IIA's Global Internal Audit Common Body of Knowledge (CBOK) survey found that 57 percent of practitioners say internal audit is fully, or almost fully, aligned to their organization's strategic plans. Another 35 percent answered that they were somewhat aligned, underscoring the subjective nature of such assessments. In addition, being aligned with strategic plans and objectives does not necessarily mean that internal auditors are involved in auditing them. Anecdotally, most CAEs admit that there can be a disconnect between what auditors report and what their clients are most interested in.

"When I go to managers' association meetings, they tend to be engaged and passionate about new digital developments, business transformation programs, and research and development projects," Polona Pergar Gujaz, internal audit consultant at 4E and president of IIA–Slovenia, says. "Internal auditors seldom talk about auditing these areas, which suggests we are not actually aligned with the kinds of managerial interests that work themselves into the business strategy."

Pergar agrees that auditors often prefer to audit the areas they know well, especially in compliance-based areas, and shy away from areas that could have a bigger impact on the organization achieving its strategic objectives—and where internal audit could potentially add more value. Admittedly, the size and maturity of audit functions can be a problem. She says the situation is better in larger departments and in the financial services sector. Yet in Slovenia, and in many other parts of Europe where Pergar works, audit functions are small, compliance related, and often have relatively low corporate profiles. Even when boards do agree in principle that internal audit should be involved in strategic work, it can be a fight to get them to speak to the CAE about the big issues, she says.

WHERE TO BEGIN

Become a Strategic Internal Auditor, a 2014 qualitative study by Walker published by The IIA, illustrates that those auditors who grasp the strategic audit nettle see tangible benefits for the organizations and departments in which they work (see "The Benefits of Getting Involved" on page 47). Getting to know the company's broad strategy can be relatively straightforward—auditors simply need to read the corporate literature and follow the relevant industry or sector in the press. Internal auditors shouldn't be put off if they find the strategy task difficult because it is a process that many organizations struggle to get right—underlining the need for better challenge and sounder assurance.

"There is a lack of definition and best practice for strategy and business planning processes, and that means a lot of companies may not know how to develop those effectively," Steven Barlow says. Barlow has been a chief risk officer in the United Arab Emirates for almost seven years and is former

"If the CAE is willing to step up and demonstrate that he or she can add value, that's a win for everybody."

Paul Walker

"Even when boards agree in principle that internal audit should be involved in strategic work, it can be a fight to get them to speak to the CAE about the big issues."

Polona Pergar Gujaz

78% of respondents say internal audit **performs well** in the attribute of business alignment, according to PricewaterhouseCoopers' 2016 State of the Internal Audit Profession Study.

CAE of Novartis, Prudential, Pearson and the U.K. Department of Energy. "Similarly, there is a lack of internal audit expertise and experience in reviewing those areas."

Barlow says internal auditors need to understand that the two biggest risks many companies face are not having an effective strategy and not executing that strategy appropriately. "Often, these two interrelated risks are not being identified or reported to the board by management, risk and compliance functions, or internal audit," he adds.

In terms of effective strategy, common pitfalls include developing aspirational strategies where the downside risks have been ignored by optimistic managers, or new product launches and initiatives into markets where the company has little knowledge and expertise. "As a result, there is often no strategic response to new entrants or to disruptive technologies that affect the dynamics of the market," Barlow says. "When those risks materialize, they can have a dramatic impact on shareholder value."

On the implementation side, he says, businesses often have only sketchy roadmaps with few milestones to show how well plans are being carried out, and can have almost no effective monitoring and follow up. If strategic objectives are not correctly linked to individual performances and incentives, the workforce is unlikely to understand how they can contribute to the business' overall strategic performance, he says.

Barlow says the CAE needs to have a dialogue with the board agreeing to a change program for the audit function to help address these issues. The new mandate should specifically align audit with the company strategy and objectives and focus its work on long-term, sustainable value related to those objectives, and the key risks and processes for managing them. Finally, that mandate should clearly position internal audit as the third line of defense so that the function can pull away from too much compliance checking—leaving that to management and the risk functions in the business.

A SEAT AT THE TABLE

Internal auditors have traditionally aligned themselves with the business' risk objectives, but that is different from being aligned with the business' strategic objectives, Greg Grocholski, vice president and CAE at the global manufacturer SABIC in Riyadh, Saudi Arabia, says. The distinction is subtle but important. It's one thing auditing perceived risks *to* strategy, it's another to truly grasp the risks *of* the strategy and processes in a broader sense.

"I've tried to align our function with the general business strategy and objectives, which means having a seat at the top table," Grocholski says. "Internal auditors have talked about

THE BENEFITS OF GETTING INVOLVED

A qualitative IIA study, Become a Strategic Internal Auditor, found that businesses in which internal audit engaged at a strategic level enjoyed a range of benefits:

- Internal audit stays connected to the business and becomes a business advisor or risk partner when it's involved in more strategic initiatives.
- Internal audit can be more proactive and get involved earlier in the life cycle of the project or strategic initiative, adding greater value.
- Enterprise risk management can be used to raise risk and strategy questions, either directly or indirectly.
- Internal audit gains valuable knowledge for the organization's future strategic initiatives when it is involved in leading-edge risk assessments in areas such as culture, the control environment, social media, or mergers.
- Internal auditors may find that new skills and additional training are necessary to engage in the increased emphasis on strategic planning.

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

this for years, and it's a challenge because it is a cultural issue, a credibility issue, and a perception issue."

Grocholski's view is that CAEs need to accept the perception problem as a fact of life and move on. He advises CAEs to act like CEOs—which implies a broader knowledge of the business than would be expected from a traditional internal auditor. Professional internal audit knowledge, adherence to The IIA's *International Standards for the Professional Practice of Internal Auditing*, and professional assurance acumen should be regarded as the minimum today, he says. Being able to think through challenges from different perspectives, having a thorough understanding of what it costs to get each product to market, and whether the business is going to achieve the right shareholder value from its initiatives is critical if internal audit is to be taken seriously.

At SABIC, Grocholski says he has been focusing on areas such as profit leakage and gross profit margin analysis. The first is designed to compare the product value margins of old and new business lines. That can reveal what added value the company derives from the billions of dollars it spends on researching new products compared to its existing lines. The second aims at getting a fine-grained understanding of the challenges of the production cycle—how fixed costs, plant depreciation and efficiency, feed stock and supply chains, energy costs, and potential liabilities affect the gross margins—and what can be done to improve the value added to the business. He says recent events at other manufacturers over emissions procedures show the need for internal audit to focus more on what happens in the production process.

To be successful, he says, CAEs need to develop the right level of what he calls intuitive analytics—the speed at which one grasps the significance of how broader business issues connect. "Imagine you're in the C-suite, where you've earned a spot, and you are in discussions with executive vice presidents, chief financial officers, and CEOs," Grocholski says. "You have to demonstrate that you can contribute to the conversation in a meaningful and substantive way that engages with them from a strategic business perspective, not from a technical, audit perspective—it's a given you can nail the audit issues when they arise. That's what it means to be a fully paid-up member of the team and deserve that seat at the table."

A LIGHTER TOUCH

On a practical level, CAEs need to re-examine their audit plans to determine how much of their focus is on strategic-level work in comparison to compliance-based audits. Striking the right balance is important. Benito Ybarra, chief audit and compliance officer at the Texas Department of Transportation in Austin, acknowledges that not all CAEs are comfortable moving into more strategic and consulting-style projects, especially after corporate disasters such as Enron and WorldCom showed how such cozy relationships can go wrong. Yet, despite the tougher regime for internal auditors brought in by the U.S. Sarbanes-Oxley Act of 2002, the *Standards* specifically allow for consulting assignments, provided everyone knows where the red lines are.

For example, the CAE may invite executives from different parts of the organization together for a workshop to discuss how the strategy implementation can be strengthened in an area where it has been found to be weak or disconnected. More detailed audit work could be needed in areas such as the quality of the decision-making processes, which can

"Truly understand what the organization's strategy is and where each executive plays into the advancement of those strategies."

Benito Ybarra

"I've tried to align our function with the general business strategy and objectives, which means having a seat at the table."

Greg Grocholski

Business **alignment** is one of the eight **core attributes** shared by well-regarded internal audit functions, according to PricewaterhouseCoopers' 2016 The Eight Attributes report.

"We added value by bringing awareness into the mix—thinking about risk and control in relation to speed of delivery."

Leen van der Plas

"There is a lack of definition and best practice for strategy and business planning processes."

Steven Barlow

be done effectively by looking at how authority has been delegated among individual executives, Ybarra says. When strategy changes, those delegations often are not updated, causing potential friction and wasted effort. Furthermore, it helps clarify the organization's appetite for risk and identify areas where added controls are required in lieu of additional flexibility and authority.

"Truly understand what the organization's strategy is and where each executive plays into the advancement of those strategies—then engage them with your recommendations based on the reviews you've done on the business' objectives and call out the gaps and challenges and have a discussion," Ybarra says. "Accept that you may not always have the best perspective, but if you don't take a risk, you'll never get there."

TAKING A RISK

Internal audit at ING Bank started realigning its work a couple of years ago, with dedicated teams working across the global business in response to new digital distribution channels and customer expectations stemming from the business strategy in the data analytics and digital audit teams. Leen van der Plas, Global Audit Division head for ING's Corporate Audit Services in the Netherlands, is part of the global leadership team that comes together at least twice a year for a strategic planning session with the CEO, audit committee, external auditors, regulators, and others to explain what is on their radars. Periodic meetings with board members and audit committee members are also on the agenda, as are a lot of interaction with top management.

"It's vital to hear things straight from the source, even if the strategy is in an early phase," van der Plas says. He builds a strategic audit program from these meetings with dedicated scopes, timelines, and resources.

"While addressing company strategy and related business objectives in the audits, we issue our audit findings with a risk rating in an overall report for each audit with an audit opinion. Dedicated project audits relate specifically to the implementation of the strategy," he says. "You have to be tough asking questions, and you need to dare to challenge, even if people find it difficult to take."

Like many in the banking sector, ING has been looking for ways to serve clients better through, for example, centralized call centers. One of ING's strategic objectives is to make its services client-centric—making the call center a one-stop shop for customers who call in and need help. Van der Plas' team highlighted, at that time, the risk that individual employees may have access to too many systems.

"This piece of work took into account both strategic objectives and controls, and our recommendations reflected that," van der Plas says. "We added value by bringing awareness into the mix—thinking about risk and control in relation to speed of delivery."

Given the obvious difficulties of businesses devising and implementing their strategies in a fast-changing world, it makes sense for someone to provide assurance that organizations are on the right track. And internal auditors are in a position to play such an important role—if they are willing to come out of their compliance comfort zones and take a risk. It is time for internal audit to rise to the challenge, before the board turns to someone else for help. ia

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

Three Lines in Harmony

LISA KOLBASA / SHUTTERSTOCK

A centralized testing model can enable the lines of defense to rely on each other's work and make audits more efficient.

Susan Burch

Many organizations have implemented a three lines of defense model with each line performing risk monitoring and testing activities. As described in The IIA's Position Paper: The Three Lines of Defense in Effective Risk Management and Control, front-line unit management is the first line of defense, risk and compliance functions are the second line of defense, and internal audit is the third line of defense. In many cases those monitoring and testing activities overlap, which can cause audit fatigue within the business units. It also takes time away from serving customers. Or in some cases, there could be gaps in coverage that expose the organization to unnecessary risks.

Each line of defense has its own monitoring and oversight responsibilities, but in many cases there are areas where the testing activities to achieve these responsibilities overlap. In these instances, organizations can benefit from ensuring each line of defense coordinates with the others to avoid performing duplicate testing or monitoring activities. Coordinating the three lines of defense can minimize audit fatigue and maximize efficiency.

MUTUAL RELIANCE

If the testing or monitoring activities performed by the first line are well-designed and executed, the second and third lines can validate and rely on what the first line does. Similarly, if the testing performed by the second line is well-designed and executed, the third line can validate and rely on the second-line testing. Benefits an organization can realize from ensuring its three lines of defense are well-coordinated include greater efficiency, cost savings, alignment with best practices, enhanced productivity, improved consistency and quality, standardized testing methodologies, and leveraging the "right" skills for specific products or lines of business. Moreover, all three lines can use software to automate the monitoring and testing of key controls and risks.

Organizations also need to be aware of challenges they may encounter when coordinating testing across the three lines. Bringing together people with the right skills, providing necessary training, and identifying technical solutions are challenges, as is ensuring the process has appropriate quality controls. Another challenge is ensuring the appropriate service-level agreements are in place so each group is clear about its roles and responsibilities, particularly with respect to a centralized testing unit.

CENTRALIZED TESTING

Coordination among the three lines of defense should enable the organization to design testing activities so that controls can be tested once and relied on by other groups to meet various regulatory requirements and needs. Organizations can leverage a shared service model to perform testing activities based on detailed test scripts. A centralized testing approach needs to reflect the roles, responsibilities, and accountabilities for each line of defense.

The "Centralized Testing Model" on this page can be used as a framework to implement more effective testing activities. Subject matter experts in each line of defense would be responsible for the more complex activities and designing the test scripts. Centralized testing groups would be responsible for conducting the detailed testing in accordance with the test scripts designed by the subject matter experts.

This model emphasizes communication, collaboration, and reliance among all three lines of defense. Organizations also should consider automating testing as much as possible and providing integrated reporting of test results. Senior management should receive consistent reporting regarding the strength of the control environment.

When considering a centralized testing model, maintaining the independence of the third line of defense

CENTRALIZED TESTING MODEL

1 First-line Subject Matter Experts

- Document processes and controls.
- Migrate some testing to second line so first line may focus on monitoring activities.
- Design quality monitoring systems.
- Conduct self-assessments.
- Build in quality control to reduce defects.
- Monitor compliance.

Centralized Testing
Conduct testing for first and second lines of defense based on detailed test scripts.

2 Second-line Subject Matter Experts

- Challenge risk assessments.
- Evaluate process documentation.
- Perform walk-throughs.
- Assess and validate control design.
- Design and develop test scripts.
- Centralize standard testing programs such as fraud.
- Assess quality of first-line monitoring.
- Improve efficiency through shared service concepts.

Centralized Testing
Conduct testing for third line of defense to ensure internal audit's independence.

3 Third-line Subject Matter Experts

- Maintain independence.
- Assess risks.
- Plan/scope audits.
- Write audit programs.
- Assess control design.
- Perform walk-throughs.
- Reperform tests/quality assurance test results.

Communication, Collaboration, Reliance

Integrated Reporting

32% of respondents say they have established a centralized testing team, while 37% have some centralized testing, according to a 2016 EY survey of Institute of International Finance member firms.

THREE LINES IMPLEMENTATION METHODOLOGY

Develop risk framework	Map testing to framework	Identify gaps and overlaps	Identify opportunities for efficiencies
» Identify regulatory requirements, best practices, standards, and guidance. » Document risks to be addressed. » Document attributes to be tested.	» Obtain test scripts from lines of defense. » Review testing policies and procedures, guidelines, and job aides. » Conduct walk-throughs to understand testing processes. » Map test scripts to risk framework.	» Analyze test script mapping. » Analyze frequency of testing. » Identify gaps (i.e., attributes not being tested by any line of defense). » Identify overlaps (i.e., duplication of testing efforts). » Analyze whether testing overlaps can be optimized.	» Analyze duplication of testing efforts, including frequency. » Determine whether duplicate testing can be streamlined. » Analyze whether testing in first or second lines could be tweaked so it can be leveraged by the third line.

is critical. Depending on the organization's structure, it may make sense to have one testing team for the first two lines, as depicted in the model, and a separate team for internal audit.

Finally, cultural maturity should be considered because organizations with more mature cultures tend to have better collaboration among business units, be proactive rather than reactive, think more strategically, and have increased consistency.

IMPLEMENTING INCREMENTALLY

An incremental approach to implementing centralized testing across the three lines of defense may allow the organization to see benefits more quickly. Standardizing processes can lead to lower organizational costs and greater predictability.

Starting with cross-functional areas, such as third-party risk, complaint handling, credit quality, payment systems, or data quality can yield quick wins and demonstrate the value of a centralized testing function. As the approach is implemented in the various risk domains, it is important to use a consistent methodology. The "Three Lines Implementation Methodology" on this page can be applied to any risk domain to evaluate testing across the three lines of defense. This evaluation can identify areas where testing can be streamlined and made more efficient as well as reveal any gaps in testing.

The first step is to develop and document the risk framework based on regulatory requirements and guidance, as well as best practices. From there, the testing performed in each line of defense can be mapped to the risk framework, which can enable the organization to identify gaps and overlaps in testing.

Once the gaps are identified, the organization can determine where the testing should take place and implement the appropriate testing or monitoring. In addition, the analysis will show areas where multiple lines of defense are performing testing or monitoring activities. These are areas where the organization can focus to optimize testing and

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

45% of respondents say they follow the three lines of defense model, with internal audit as the third line, but 10% say the lines are blurred, the Global Internal Audit CBOK Practitioner Survey notes.

improve efficiencies to minimize audit fatigue. The organization should analyze whether testing conducted by the first or second line can be refined so it can be relied on by the second or third line of defense. Using a consistent methodology can help ensure the implementation process is repeatable.

BEST TESTING PRACTICES

Organizations that are thinking about implementing a centralized testing model should leverage lessons learned by others who have gone down this path. Some of the leading practices for coordinating or centralizing testing in the three lines of defense include:

- » Use subject-matter experts to support risk identification, assessment of control design, and development of test scripts.
- » Leverage automation through continuous monitoring routines that run regularly.
- » Use advanced data analytics to identify patterns and trends.
- » Empower small, nimble teams with advanced testing capabilities and tools to perform targeted reviews in high-risk areas in off-cycle periods.
- » Coordinate acquisition of data among the three lines of defense to reduce the impact on internal resources within the business lines.
- » Leverage the organization's off-shore resources to perform routine, high-volume testing, subject to appropriate oversight.
- » Leverage contingent staff and consultants to supplement the testing staff when special reviews or seasonal spikes demand increased testing efforts.

Although adopting these practices to coordinate testing activities across the three lines of defense may take considerable effort, they may yield great rewards. This effort can help the organization validate that key controls are being tested and streamline testing across the three lines. Such gains can reduce audit fatigue on the front-line units so they can focus on serving customers and improve efficiencies in second- and third-line units. This can allow internal audit to provide broader, more in-depth, and complete coverage of risks and controls.

SUSAN BURCH, CIA, CRMA, CFE, CISA, *is a manager at Grant Thornton LLP in Raleigh, N.C.*

Signature Audits

MERCEDES-BENZ USA

Hans Buehler and Arnaud Ruiz

Audit client expectations have risen steadily over the past several years, requiring internal audit to increase its value delivery and become more relevant to day-to-day business. Yet practitioners often struggle to meet these expectations, as reported in a 2016 KPMG report, Seeking Value Through Internal Audit. Only 10 percent of the financial executives and audit committee chairs surveyed agreed that internal audit adequately identified and responded to emerging risks. Respondents indicated that audit results too often confirm concerns already identified by management instead of identifying new issues and emerging risks. Some chief audit executives have been quick to explore new service and delivery models that can provide value to stakeholders beyond assurance, leading to the development of advisory services and consultative reviews. But these efforts have not always considered how to improve existing audits.

To address this challenge, internal audit teams at German automaker Daimler have looked for ways to improve assurance services and tap into the unrealized value of its process audits. Although the annual audit plan offered numerous ways to increase value to the organization, internal

Daimler's audit function adds significant value to engagements by incorporating a unique methodology focused on innovation.

audit sought to explore new ways to add value within the framework of existing audits. To identify and exploit new opportunities, the team launched a program called Signature Audits, aimed at increasing internal audit's contributions during regularly scheduled client engagements.

LAUNCHING THE PROGRAM

The audit team introduced its Signature Audit methodology by first selecting an engagement that offered a suitable environment to pilot the concept. Daimler was poised to launch new technologies and services considered strategically important to the organization and monitored by top management. To identify unknown risks and potential workarounds to processes being implemented, an unconventional audit approach was required. The audit team needed to look beyond existing

DAIMLER TRUCKS NORTH AMERICA

client policies and procedures to capture emerging risks and resolved to deploy audit techniques that are typically used less frequently during traditional processes. Practitioners used a hands-on approach that involved re-performance of controls or simulations such as mystery shopping—where the identity and purpose of the customer is not known by the group being evaluated.

In another type of simulation, two of the auditors created a fictitious account consisting of customer information from one auditor and bank account information from the other. The practitioners used this technique to determine whether the controls to validate customer identities would pick up the mismatched personal information (whereas in a regular, non-signature engagement, auditors might just verify that the customer's personal information was appropriately captured). Internal audit's objective was to assess real-life scenarios as opposed to conducting paper-based assessments that often rely solely on the audit of existing policies and their implementation.

The results of the Signature Audit pilot exceeded expectations. Findings captured critical risks that weren't identified by existing processes and required senior management to rethink certain aspects of the service to be deployed. The added value from the assessment became obvious as senior management immediately deployed corrective actions.

A DIFFERENT KIND OF AUDIT

Although Signature Audits resemble traditional process audits in many respects, fundamental differences exist between the two approaches. Signature Audits usually require more preparation, more resources, additional training, and a unique mind-set—to implement them, auditors need to be innovative, curious, and creative. For example, when Daimler auditors assessed controls around cargo access security within the company's supply chain, they knew that a review of delivery slips would not suffice. On paper, controls seemed to be in order—all inspection forms were completed and signed, without any deviation from normal procedure. But when the auditors decided to follow delivery trucks, track their routes, and conduct random checks on cargo security, different results came to light. Asset counts differed from what was documented, and cargos were discovered unlocked. The auditors found that key aspects of the process had been circumvented—something a traditional audit may not have captured.

SELECTION AND PREPARATION

Not all process audits are appropriate candidates for the Signature Audit approach. Signature Audits have a better chance of success, and a more significant impact, when applied to strategic areas with a significant level of complexity. Moreover, the approach is often particularly effective if the strategic area involves new processes, such as the deployment of a new service or a new technology.

Signature Audits often require unique preparation, including the consultation of experts in the audited area who can help design creative test scenarios. Auditors may also need to improve their knowledge of the process, product, or service under review. They should be prepared, as well, to take a certain amount of risk. Creative audit techniques, such as the use of penetration testing tools or social engineering techniques, may involve a degree of deception. Senior management and the legal department should authorize internal auditors to perform these types of procedures, and the auditors should immediately inform these groups of any critical findings. For example, if auditors successfully manage to compromise a system's security, senior management must be made aware of the activities

96% of respondents to the Deloitte Innovation Survey consider innovation to be one of their top five strategic priorities; more than 20% consider it their No. 1 priority.

so they can initiate corrective actions without delay.

Extensive reconnaissance efforts may be conducted that require additional resources, such as laptops and penetration-testing software. Benchmarking research and market analysis may also be required, and travel could involve visits to multiple locations outside the audit client's office. Significant travel may be necessary, for example, if auditors visit similar plants in different countries to compare processes and identify best practices before audit fieldwork begins.

FIELDWORK

The performance of fieldwork in real-life conditions, as opposed to a paper-based assessment, is an essential component of Signature Audits. When reviewing a three-way match, for example, Daimler's auditors will consider the end-to-end accounts payable process and physically observe the receipt of goods instead of solely relying on the system data. Or, when assessing a warranty claim process, auditors will actively generate warranty claims in production and simulate real-life scenarios. Auditors can engage guest auditors with expert knowledge to help create these simulations, or hire consulting or other specialized expertise to accompany them during audit preparation and fieldwork.

Daimler's auditors are encouraged to identify creative ways to complete test work, using innovative tools and resources. Examples include unannounced site inspections, simulations of real-life conditions, social engineering, exploiting system vulnerabilities, and data analytics. In one instance, the auditors exposed a security flaw by creating a fake employee with full administrative rights. Using these credentials, they were able to add, delete, and manipulate data, as well as delete records of certain inventory entirely from existence. Although such techniques are occasionally used during regular process audits, Signature Audits rely on them extensively.

During Signature Audit fieldwork, practitioners often seek to circumvent processes as opposed to testing process effectiveness. For example, while auditing a new mobile application, internal audit decided to test a phone hotline established for customers experiencing difficulties. Signature Audit techniques applied to the call center in charge of the hotline revealed that the app's authentication controls could be easily bypassed by calling the center. Similarly, penetration tests on the call center systems revealed additional vulnerabilities and severe control weaknesses, leading to a significant change in the design of the service.

Daimler's auditors are encouraged to identify creative ways to do test work, using innovative tools and resources.

REPORTING

The reporting phase of a Signature Audit also features key differences from a regular engagement. Presentation of results, for example, is rarely done using standard PowerPoint presentations or Excel templates. Instead, communication relies on real-world demonstration of the concerns identified. The process may entail a field visit with the client and senior management to observe certain issues in person. Or it can be done through the use of audiovisual resources, such as playing video or audio recordings, performing live simulations (which are often effective when auditing IT and engineering), or displaying pictures of audit evidence.

Offering tangible evidence is an effective way to engage the client

MERCEDES-BENZ USA

Most **stakeholders** see internal audit as contributing **significant value**, yet they are still expecting more, according to PwC's 2016 State of the Internal Audit Profession survey.

and communicate value to stakeholders—something that Daimler internal audit has confirmed with client feedback on its Signature Audits. Concrete audit results pointing to proven deficiencies and impact, as opposed to identification of control gaps that present a hypothetical risk, can lead to significant improvements in the acceptance of audit results and remediation efforts. Daimler's auditors observed this effect when they reported on information security vulnerabilities found in an online service—instead of simply reporting on control gaps in the vulnerability management process, the team showed senior management a 30-minute demo highlighting the damage that could occur. After seeing the ease with which vulnerabilities could be exploited, management took corrective actions immediately.

Management's reaction to the Signature Audit experience was typical—surprise at first and then ultimately, appreciation. Showing clients actual risk instead of simply telling them about risk potential elicits a much higher degree of engagement and helps increase the likelihood that corrective actions will be taken.

A CULTURE OF INNOVATION

Implementing Signature Audits provides an effective vehicle to communicate the value of internal audit to the organization, including senior management and the audit committee. It provides an opportunity to showcase the audit team's ability to advance the organization's strategic goals and contribute to the identification and assessment of emerging risks. The focus on exploiting control gaps to illustrate the impact of deficiencies creates stronger buy-in from audit clients, improved remediation results, and increased trust from internal audit stakeholders. It can also lead to additional demand for audit services as stakeholders realize the value of this approach and decide to engage the audit department in other similar audits.

The Signature Audit concept also provides an opportunity to create a culture of innovation within the audit team. The explorative nature of Signature Audits offers a significant learning experience for practitioners as well as the ability to unleash their creative potential—it gives them a chance to ask what they would do differently to improve a product or service. As a result, auditors gain a more direct connection to organizational performance, which can increase their

Showing clients actual risk instead of telling them about risk potential elicits a much higher degree of engagement.

commitment and ability to deliver results. It can also improve the relationship between the internal audit function and other departments in the organization, due to the collaborative use of guest auditors during the preparation and fieldwork phase, and it helps increase internal audit's ability to retain and recruit talent by fostering a positive image of the function. The methodology can lead to numerous enhancements that benefit the audit department, promote business improvement, and enhance internal audit's stakeholder value proposition throughout the business. Ia

HANS BUEHLER, CIA, *is senior manager, Audit, North America, at Mercedes-Benz Financial Services in Farmington Hills, Mich.*

ARNAUD RUIZ, CISA, *is manager, Audit, IT, North America, for Mercedes-Benz Financial Services.*

TO COMMENT on this article, **EMAIL** the authors at hans.buehler@theiia.org

BY DAN CLEMENS & RICK NEISSER EDITED BY MARK BRINKLEY

LEVERAGING RELATIONSHIPS

Internal audit implemented a four-step cycle to help ensure a healthy corporate culture.

Today, whenever corporate fraud or scandal hits the headlines, no player is held harmless. Along with everyone else involved, internal auditors will be asked, "What did you know, and when did you know it?" Internal audit departments must continue to ask themselves how they can better help the organization maintain a healthy, ethical culture.

Several years ago, Farmers Insurance Internal Audit addressed that question by putting in place its Relationship Management process. This four-step cycle has enabled us to keep our fingers on the pulse of the company's culture by sitting down at regular intervals with the top leaders to review their visions, values, and strategies. The process has afforded the means of reassessing company risk and adjusting our audit plan to cover those risks timely.

Our relationship management cycle has played a big role in conforming to IIA Standard 2010: Planning, which states: "The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals."

As the diagram on page 63 shows, the relationship management cycle consists of:

1. Conducting periodic meetings with the top 150 leaders.
2. Reassessing risks based on those meetings.
3. Adjusting the audit schedule to meet the changing risk environment.
4. Updating the audit universe to ensure adequate coverage in all key areas.

Step one of the cycle—the relationship management meetings—is the engine that drives the other three steps in the process and is the focus of this article. The benefits of the meetings are multifold, as they enable us to:

- Promote a relationship of trust, mutual respect, and partnering between company leaders and internal audit.
- Systematically identify business strategies, objectives, initiatives, risks, and controls.
- Update our audit universe and schedules to reflect emerging risks and business needs.
- Grow our talent by having audit managers, and often auditors, participate in the meetings.
- Provide value and insight to our customers through these meetings and the projects that result from them.

For this process to work, relationship management owners must be adroit and capable. The owners are audit staff who are matched to company leaders based on their expertise, areas of specialty, and interests. Take, for example, an audit manager who specializes in underwriting. It makes sense to assign him as relationship management owner to the Underwriting

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

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

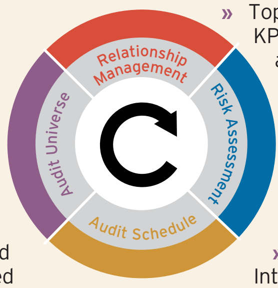
FARMERS INTERNAL AUDIT RELATIONSHIP MANAGEMENT (RM) CYCLE

Audit Universe

- The Farmers audit universe maps all key areas of the business, related risks, and prior/planned audits.
- The universe is continually updated based on changes to company organization, audit risk assessments, and audit schedule.
- RM often triggers changes to the universe.

Relationship Management

- Internal Audit periodically meets with executives and heads of business units.
- Topics include business strategy, KPIs, initiatives, emerging risks, and audit schedule.
- Meetings are documented in an RM database, and results shared with the senior audit leadership team.



Audit Schedule

- The audit schedule is reviewed quarterly to reassess proposed and planned audits.
- Scheduled audits may be moved or pushed back.
- New audits may be scheduled, as well as advisory projects requested by Farmers management. The audit plan is revised.

Risk Assessment

- Following RM meetings, Internal Audit revisits and updates its companywide risk assessment.
- Business strategies, emerging risks, and initiatives can all impact the risk assessment.
- Key risks include financial, strategic, compliance, and operational.

head. The commonalities between staff and leader can go a long way toward creating mutual relationships of trust, rapport, and respect. Without that, the cycle will fall short.

Relationship management owners are responsible for all aspects of the meetings. Planning and scheduling the meetings may require tenacity and persistence in tracking down leaders who are often on the road. Conducting the meetings requires the use of effective soft skills to draw the leaders out so they are forthcoming and frank. They should feel comfortable enough not only to share their strategies, but also to reveal the obstacles and threats to achieving them. Relationship management owners' notes of the meetings must be accurate and complete, as they will often provide the springboard for discussions with senior audit leadership on what was learned.

The relationship management owner sets the agenda for the meeting. Agendas will cover strategy, objectives, and business plans and the risks that threaten them. If warranted, past audit results also will be covered. The audit schedule will be reviewed to verify content and timing of planned audits. If the leader is new or unfamiliar with the audit process, we will add our charter to the agenda so we can cover our principles.

The frequency with which relationship management owners meet with company leaders depends on several factors, including: leader experience, size and complexity of the operation, ongoing changes or initiatives, and past audit results. For example, Claims is Farmer's largest department and the pace of change within it may warrant meeting with its leaders three or four times a year. Meeting once a year may be sufficient for smaller departments or those with a slower pace of change. Relationship management owners confirm the meeting frequency with senior audit leadership.

Before the meetings, relationship management owners will email the agenda to the leaders, inviting their input on areas to discuss. The email will often include the ongoing and planned audit schedule for the leaders to review. Whenever possible, the relationship management meetings will be held on site. Relationship management owners will often include other auditors who have an interest or are specializing in that area of the company. This provides an opportunity to grow our talent, as these auditors observe and learn from participating. One of those auditors will usually be the scribe, and after the meeting send the notes to the relationship management owner for review and distribution. Meetings usually run about one hour. All meeting records are stored in a database.

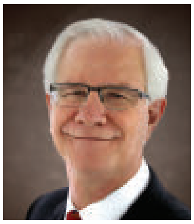
Each quarter, our senior audit leadership team meets to review and adjust the audit plan. This is when our relationship management meetings pay off. The relationship management owners will share results of those meetings, and, in particular, focus on changes that have occurred to the risk landscape of the department in question. Reassessing risks, the leadership team will adjust the audit plan, moving up some audits, pushing back others, and, in some cases, setting up new audits. This is also the time when the leadership team will consider requests made by leaders during relationship management meetings for us to provide consulting services.

While we may attribute organizational failures to things like fraud and poor leadership decisions, culture is really at the crux. Bad decisions stem from an unhealthy culture. Our relationship management cycle puts us in a unique position to help ensure our company's culture remains healthy. Ia

DAN CLEMENS, CIA, *is head of Internal Audit Planning and Operations at Farmers Insurance in Phoenix.*

RICK NEISSER, CIA, CISA, CPCU, CLU, *recently retired as an audit consultant at Farmers Insurance in Woodland Hills, Calif.*

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



BY J. MICHAEL JACKA

A REAL ELEVATOR SPEECH

Brief interactions sometimes provide a perfect opportunity to extol the virtues of internal audit.

When we are honest, we have to admit that internal auditors don't always enjoy a positive reputation. Partly, unfavorable perceptions exist because people don't know what we do. And unfortunately, they also stem from people who think they do know what we do. So we always have to be ready to share our side of the story—sometimes at a moment's notice.

On my way to speak at a recent IIA–Fort Worth chapter meeting, I struck up a conversation with someone in an elevator. When I mentioned I was giving a presentation, he asked what I was speaking about. Fearful of the response I was sure to receive, I told him, "Internal audit." He did not disappoint, forming a cross with his fingers and jokingly—I hope—saying, "Keep away!"

I laughed. "Don't worry, I'm not one of those auditors," I said. "I don't try to find people doing things wrong; I try to help people do their jobs better."

I could tell he didn't believe me, but he also seemed willing to give me the benefit of the doubt (if for no other reason than hoping this might free him from being audited while on the elevator). And at that point I had a sudden realization. "You know," I said, "they always say you're supposed to have an elevator speech. I guess I just gave mine. Did it work?"

He laughed. "Well, at least it was short."

Yes, I actually got a chance to give an elevator speech. And I got to give it on an elevator. Did I make a difference? Did this person come away with a new perspective on internal audit? I really can't say, but I learned three things.

First, elevator speeches really happen. Our days are filled with brief interactions and, sometimes, those interactions can provide an opportunity to talk about the value of internal audit.

Second, elevator speeches need to be short. That means we must be able to express the value of internal audit in a succinct way that resonates with the listener.

And third, even a few seconds can spark a change in someone's perceptions. My hope is that this gentleman remembers his conversation with an internal auditor (if he remembers it at all) as a quick interaction that gave him new information—perhaps enough to keep his fingers from forming a cross next time.

I like to think of this experience as a little nudge. A little nudge can make a difference, and enough little nudges can start a groundswell. In turn, that groundswell can lead to better understanding of internal audit's value among people everywhere.

So, in Fort Worth, Texas, because of an elevator speech delivered in an actual elevator, one person's perspectives about internal auditing may have been nudged just a little. Who have you nudged today? 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

Eye on Business

IN THE FACE OF NATURE

Comprehensive recovery strategies enable organizations to respond more quickly and cohesively following a disaster.

DAMIAN WALCH
Managing Director, Risk and Financial Advisory
Deloitte

ROBERT W. KASTENSCHMIDT
National Leader, Risk Advisory Services
RSM US LLP

When considering natural disasters, what are the biggest risks to organizations?
KASTENSCHMIDT Unlike events that impact only the organization, natural disasters can affect an entire local area or even a region. As a result, natural disasters have the potential to impact a large portion of the organization's staff, making them unavailable to participate in the recovery effort. Such events also often impact the organization's vendors, business partners, customers, etc.—all of which are factors that may significantly increase the impact of a business disruption event and the nature of the required response.
WALCH Generally speaking, the biggest natural disaster risks in the U.S. are tornadoes, hurricanes, and floods. While the U.S. hasn't seen a significant earthquake in many years, Ecuador, Italy, and Taiwan all experienced catastrophic earthquakes resulting in major loss of life and business disruptions with global impact. No matter the form of the natural disaster, they all pose possible major disruption to employee health, safety, and housing—not to mention disruption to business partners and supply chain participants.

What are the greatest risks to organizations of prolonged downtime?
WALCH Disruption of normal operations due to prolonged downtime can slow communications, ultimately resulting in brand and reputation damage that leads to customer loss, C-suite and board involvement, negative media coverage, and shareholder value loss.
KASTENSCHMIDT Being unable to adequately recover key systems and business functions timely can expose an organization to any number of unacceptable consequences. Beyond the more immediate impacts the organization may incur during downtime, such as lost revenue and additional expenses, one of the more serious long-term concerns is the potential erosion of hard-earned market share. After working for years or even decades to develop a solid market share, an organization can see it erode quickly if it is not able to meet the needs of its customers following a disaster. To keep their own businesses operational, even the most loyal customers may turn to a competitor to obtain required products or services—and once they've departed, they may never return.

What types of staff protections should be in place?
KASTENSCHMIDT A comprehensive recovery plan must consider situations that substantially limit the availability of the organization's staff. To mitigate the risk associated with a limitation

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

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

of employee availability, organizations should factor contingency staffing considerations into their recovery plans. Such considerations may include staffing redundancy or overlap for critical functions, formal cross-training of key activities, thoroughly documented standard operating procedures, and arrangements with third parties to provide required assistance when needed.

WALCH Employee protections should include basic protections like the ability to shelter in place and evacuation plans, training on how to respond in a crisis, and resources available to them in the unlikely event of widespread disaster. Companies should have simple playbooks to instruct employees, notification systems, and training programs that include simulations.

What safeguards should organizations have to protect against data loss?

WALCH Having a strategy for data backup, off-site storage, and recovery is considered mature by many business leaders. However, the exponential growth in data combined with interdependencies between systems and applications has made that more difficult. Companies of all sizes are struggling to protect against storage corruption, data leakage, and ransomware attacks. Special precautions some companies are leveraging include taking frequent data snapshots to minimize data loss, moving data off site or far from an incident location, and creating isolated networks for data backups to protect against malware attacks.

KASTENSCHMIDT Many organizations have adopted system replication or similar technologies to minimize the data that would be lost if their primary systems were destroyed and they were forced to restore the systems in an alternate environment. However, despite these modern technologies and the small window of potential lost data, organizations still must consider how lost data and transactions would be replaced, reconciled, etc., following a disaster, through using a backup solution that considers various factors such as potential data corruption, geographic separation, and security threats. While the potential data loss, or recovery point objective, may have decreased substantially in recent years, few backups are truly "real-time" copies, and losing even a few minutes' worth of data/transactions can be devastating.

Losing even a few minutes' worth of data/transactions can be devastating.

Why is a coordinated response important?

KASTENSCHMIDT Following a disaster, time and resources are both severely constrained. As a result, efficiency is paramount in executing an effective response/recovery effort. Without thorough coordination across the response process, participating teams and individuals may unnecessarily duplicate tasks, while other key activities may be overlooked. Furthermore, key elements of the response process—including internal and external communication—can be inconsistent or even contradictory, if not coordinated across the organization. Coordination of the response effort can not only allow the organization to recover quicker and more successfully, but it can also help to alleviate some of the impacts that can be encountered as a result of the event.

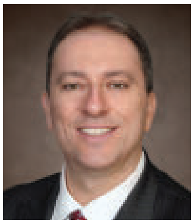
WALCH We have seen strong coordinated response and recovery efforts help decrease the financial and reputational impact of prolonged outages, disasters, and incidents. A good response requires consistent information synthesis during the event. Information sharing among executives in communication, legal, operations, and human resources is vital to the success of response. Coordinated response is required for transparency to shareholders, stakeholders, and customers in the event of a natural disaster or negative event.

What lessons can organizations learn from past large-scale disasters?

WALCH As with most things, having a plan in place is better than not. Companies that analyze their critical business processes and develop appropriate resiliency strategies to protect them are often able to respond in a more measured and cohesive manner during the hours immediately following a disaster. Planning efforts can include creating and thinking through crisis response playbooks and strategies, as well as war gaming or simulating crisis events to train leaders, employees, and sometimes business partners how to respond.

KASTENSCHMIDT In the aftermath of major events such as Superstorm Sandy, many organizations determined that the way they have traditionally approached disaster recovery plan testing was simply not adequate. In particular, organizations discovered that making assumptions—or cutting corners—in their testing prevented them from uncovering severe deficiencies in their recovery strategies and plans. Although effective testing has always been an important part of the recovery planning process, some previous large-scale disasters have only increased awareness of the importance of assuring that such testing is truly realistic. Ia

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



BY DAVID O'REGAN

WE CAN'T CODIFY EVERYTHING

Internal audit knowledge should not become subordinate to methodological demands.

Internal audit's professionalization is largely the result of codified activities. Established, credible paraphernalia of professional practice, including comprehensive standards, practical guidance, rigorous certification requirements, and a code of ethics, form the foundation of internal auditing. Steadily increasing public recognition and respect for internal auditing surely exists in part due to this robust structure. Nonetheless, as the profession continues to mature, we have reason to be cautious. Once a critical mass of standards and advisory material has been reached—and it may perhaps already have been reached—we should pause to avoid being stifled by instructions, bureaucracy, and over-codification.

To a large extent, unspoken assumptions bind internal audit professionals together in their common endeavors. Arguably, a large part of a profession's wisdom arises from experience and knowledge that are too deep to be articulated. Codified guidance cannot capture the full range of professional activity that involves wisdom and sensitivity.

Explicit instructions and bureaucratic literalism can create the illusion that what really matters in professional activity can be captured entirely in written form. Moreover, it implies that professional practice must be based solely on this established guidance. The distinguishing features of many professions—a physician's bedside manner, an architect's aesthetic sensitivity, and the acerbic rhetoric of a courtroom lawyer—cannot be codified in rational blueprints.

We may distinguish for our purposes among three types of knowledge: knowledge *that*, knowledge *how*, and knowledge *what*. The auditor may know *that* a procurement process aims at an optimal decision on expenditure, and he or she may know *how* the details of the process unfurl. The auditor's professionalism becomes truly apparent, however, with the third level of knowledge: he or she knows (through observation, logic, and judgment) *what* to conclude on the status of the risks and risk-mitigating internal controls observed. Attainment of this third type of knowledge is easier to recognize than to define, and it is founded on education, practical experience, and wisdom.

Sometimes the internal audit profession, like a silkworm, appears to be spinning around itself a cocoon of instructions and codified practices. If the focus of internal auditing shifts further from knowledge and experience to compliance with instructions, the outcome might be a subordination of the search for truth to the satisfaction of methodological demands. Furthermore, there is something eerie in the notion that the accumulated knowledge of internal auditors can be adequately preserved in a code of established practice. Creativity may be dismissed as infidelity to codified instructions. Professional guidance needs to set out the essentials while providing space for our practical judgment to flourish. Otherwise, we may be perceived as a profession characterized by box-ticking compliance, rather than by wisdom. Ia

DAVID O'REGAN, CIA, FCA, *is auditor general in the Office of Internal Oversight and Evaluation Services at the Pan American Health Organization in Washington, D.C.*

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

Sharpen Your Financial Services Acumen

With an ever-changing financial services landscape, the demand for top talent and acumen in the financial services industry rises. Stay on top of your game and establish your credibility with The IIA's suite of resources for financial services internal auditors.

Financial Services Audit Center

Influential. Impactful. Indispensable.

Join the FSAC today and gain access to exclusive thought leadership, regulators, industry leaders, and practitioners.

Financial Services Exchange

Sept. 18–19 | Renaissance Downtown Hotel / Washington, D.C.

Attend the premier financial services knowledge sharing experience that brings together regulators, industry leaders, and internal audit practitioners to connect, collaborate, and evolve.

Register before July 24 to save US$100!

Certified Financial Services Auditor® (CFSA®)

Earn your CFSA® and set yourself apart from peers by demonstrating your commitment to the profession and establishing your financial services internal audit credibility.

Learn more today!
www.theiia.org/FSAC

The Institute of Internal Auditors

Financial Services™ AUDIT CENTER

2017-1663