FEBRUARY 2019

A PUBLICATION OF THE IIA

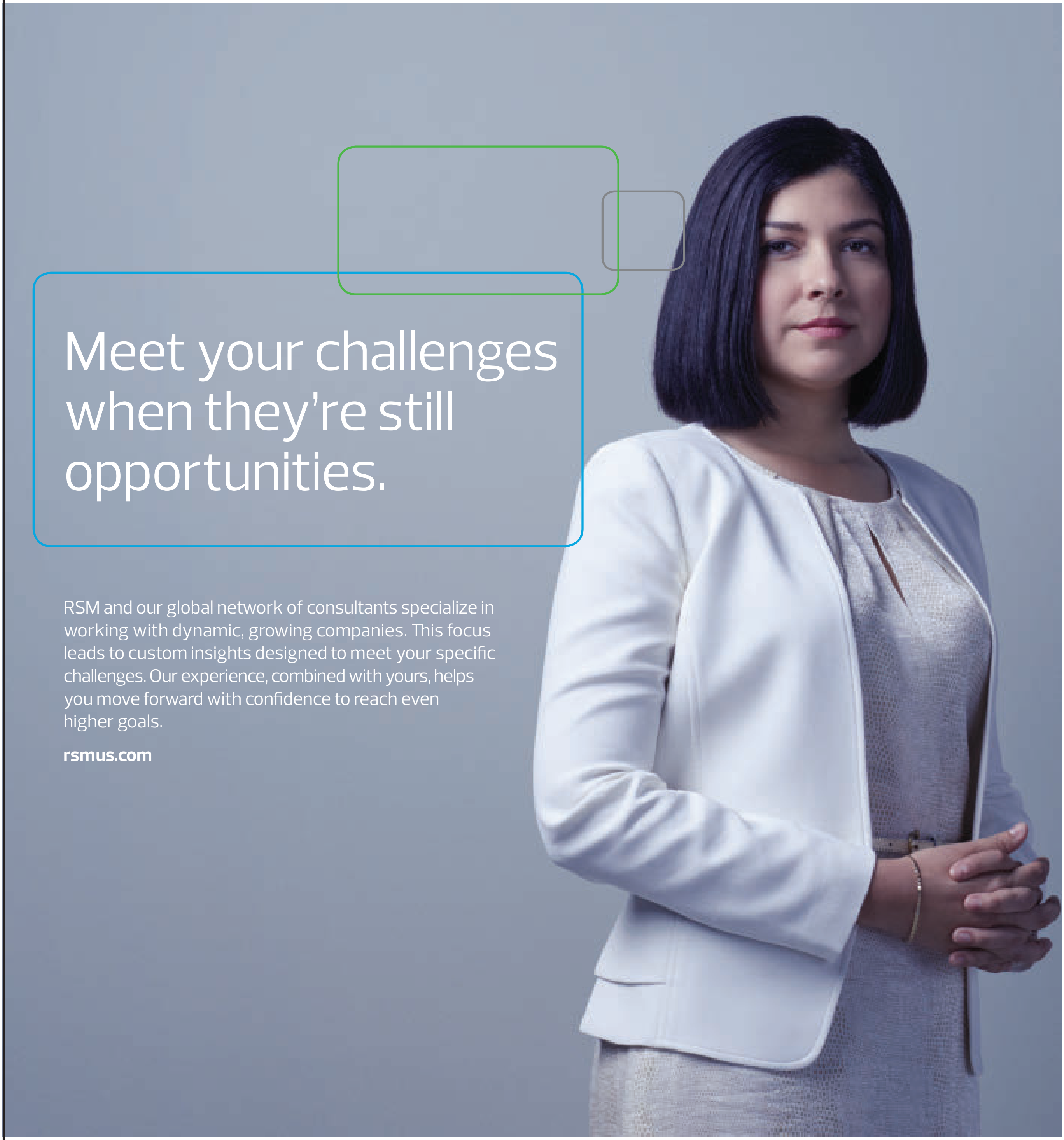
Ia

INTERNAL AUDITOR

TRIALS AND TRANSFORMATION

Ten years after the global economic crisis, the internal audit profession is strong and ready to take on new challenges.

Richard F. Chambers
IIA President and CEO



RSM and our global network of consultants specialize in working with dynamic, growing companies. This focus leads to custom insights designed to meet your specific challenges. Our experience, combined with yours, helps you move forward with confidence to reach even higher goals.

rsmus.com

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

RSM US LLP is the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

“Consultants” can be replaced with the following specialties if necessary: Financial Advisory, Valuation, Forensic Accounting, Litigation, Technology and Management Consulting Advisors, ERP and CRM, Infrastructure, Risk Advisory, Security and Privacy, and Internal Audit. “Middle market companies” can also be replaced by “dynamic, growing companies” when needed.

IIA Training Stations
IIA ONDEMAND

Ia
INTERNAL AUDITOR

FEBRUARY 2019 VOLUME LXXVI: I

FEATURES

Ia
INTERNAL AUDITOR

FEBRUARY 2019 VOLUME LXXVI: I

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Agile Planning With today's rapidly shifting business priorities, established audit plans may need to be reshuffled quickly to meet stakeholder demands. Are CAEs up to the challenge?

Assurance in the Privacy Regulatory Age Internal audit can help ensure the organization complies with the new wave of privacy regulations.

Disruptive Leadership Watch Citigroup Chief Auditor Mary McNiff explain the need for audit leaders to practice disruption, emphasizing its key role in talent management and innovation.

Fleecing the Crowd Despite crowdfunding's good intentions, some campaigns may be raising money for fraud.

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. Copyright © 2019 The Institute of Internal Auditors Inc. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in 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. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

COVER AND PREVIOUS PAGE: PHOTOS BY DOUG SCALETTA; THIS PAGE, TOP: HAKINMHAN / SHUTTERSTOCK.COM, BOTTOM: RA2STUDIO / SHUTTERSTOCK.COM

Wolters Kluwer

When you have to be right

Please join TeamMate and ArcelorMittal for an engaging presentation at the IIA GAM Conference

Session Name, Date, and Time:

Delivering Greater Value through Global Combined Assurance

Monday, March 11 from 2:00pm - 3:00pm

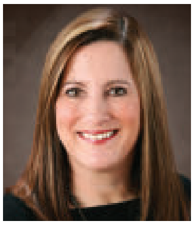
Description:

Many organizations are striving to create a combined assurance process that is pragmatic, collaborative, and efficient. Getting all parties on board and working towards this common goal can be challenging without a clear vision and a well-defined process on how to get there. Learn how one Fortune Global 500 organization has not only implemented a combined assurance strategy, but also created both time and cost efficiencies along the way.

Presented by:

Wolters Kluwer | ArcelorMittal

Sign up to receive a Sneak Peek of the presentation ahead of GAM and a full copy afterwords at **www.TeamMateSolutions.com/GAM19**



10 YEARS ON

I look back at late 2008 and early 2009 as the most difficult time of my 18-year career with The IIA. It was the one time I was forced to let team members go, and to watch friends and co-workers lose their jobs through no fault of their own. At the time, the global economic crisis was making its way through organizations, and The IIA was not spared. The Institute was forced to part with more than 40 employees despite efforts by leadership to steady the ship.

As that difficult time was beginning, The IIA's Board of Directors brought in Richard Chambers as The Institute's ninth president. Chambers, along with the Board, worked closely with IIA staff members to identify areas where The IIA could cut costs and grow revenue. "Those early months of 2009 were really spent working collaboratively," Chambers says, adding that the process "really exemplified the very best of who we are."

Ten years on, I had the opportunity to sit down with Chambers at The IIA's Headquarters in Lake Mary, Fla. He reflected on those challenging days, discussing how The IIA and the internal audit profession responded to the financial crisis and how both have grown in scope and influence since then. In "Trials and Transformation" (on page 24), Chambers notes, however, that there is much room for improvement when it comes to internal audit's value proposition. For example, he points out the need for practitioners to fully embrace the *International Standards for the Professional Practice of Internal Auditing* and learn to provide foresight on risks to the organization.

In "The Forward-looking Auditor" (on page 60), Shawn Stewart of Grant Thornton and Sandy Pundmann of Deloitte take the internal audit foresight discussion further, delving into just what it will take for internal auditors to succeed in this area. "If successful, internal auditors have an opportunity to inform and shape the critical decisions that their management teams must make," Stewart says.

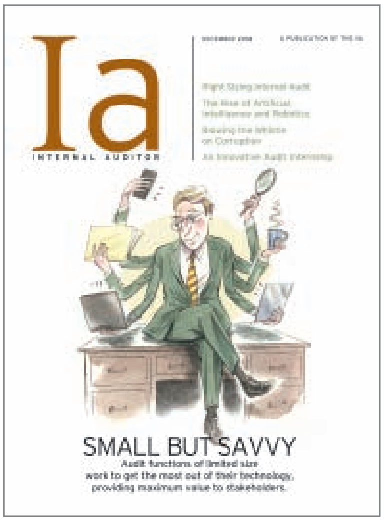
Among those decision-makers is the audit committee, which is the focus of *Internal Auditor*'s new department, "Board Perspectives," on page 57. We have revamped and renamed "Governance Perspectives" to focus on the expectations of internal audit's stakeholders—the board and audit committee. The department is written from the perspective of the audit committee, featuring committee members sharing their views on how internal audit can provide value to them and the organization. These leaders also will discuss the audit committee's oversight responsibilities, ways to align internal audit with the audit committee, and timely business events in which audit committees and internal audit should be involved. Matt Kelly, editor and CEO of Radical Compliance, is the author of the new department. Let us know what you think!

Anne

@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.


Ia
INTERNAL AUDITOR
SMALL BUT SAVVY
Audit functions of limited size work to get the most out of their technology, providing maximum value to stakeholders.

The Danger of Underthinking

I recognize a number of these issues — as I am sure many auditors do — and they are some of the reasons audit is not as value adding and productive as it could be. However, there is an irony when we hear of a book about overthinking that is followed by seven things not to do. In other words, arguably overthinking, itself.

As I see it, we need to be wary of all thought traps — overthinking and overcomplicating things — but we also need to be wary of underthinking: doing superficial work, not making our work relevant to the business, and not getting below the surface of what causes issues to recur (e.g., root causes). It takes brains, teamwork, and good communication to get the right balance of thoughtful but practical and rigorous but not overcomplicated. Let's think critically about any book with an overly simplistic answer to all our challenges.

J. PATERSON *comments on Murray Wolfe's "Breaking Free of Mental Traps" (December 2018).*

Being Relevant to Management

I think the key is not for internal audit to focus on the biggest risks, but, instead, to focus on the top value creation and preservation objectives using an objective-centric risk assessment that links to strategy and performance. That will immediately make audit's work more relevant to management, particularly if management's compensation is linked to performance. If management and the board won't allow internal audit to look at value creation, at least use an objective-centric risk assessment for the more traditional value preservation objectives.

TIM LEECH *comments on the Chambers on the Profession blog post, "'We Are Here to Help You': Managing Relationships When Management Is Skeptical" (InternalAuditor.org).*

Fear of Organizational Politics

From my observations, rather than ignoring organizational politics due to professionalism and ethical reasons, most of us are, in fact, afraid to become actively involved in it. Maybe because there is an inverse correlation between strong analytical skills and strong interpersonal ones. Whatever the reasons may be behind nonparticipation in organizational politics, it is a fact that our achievements are significantly affected by our skills to understand the organization's "shadow activities" and use their dynamics. Of course, my comments refer only to positive politics.

ELTON XHAFA *comments on the From the Mind of Jacka blog post, "I Hate Politics" (InternalAuditor.org).*

Ia
INTERNAL AUDITOR
FEBRUARY 2019
VOLUME LXXVI:I

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design

PRODUCTION MANAGER
Gretchen Gorfine

CONTRIBUTING EDITORS
Wade Cassels, CIA, CCSA, CRMA, CFE
J. Michael Jacka, CIA, CPCU, CFE, CPA
Steve Mar, CFSA, CISA
Bryant Richards, CIA, CRMA
James Roth, PHD, CIA, CCSA, CRMA
Charlie Wright, CIA, CPA, CISA

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")

Digital capabilities are executives' top risk... Low cost for cybercriminals... Stakeholders' internal audit expectations... "Mules" and money laundering.

Update

AI STEWARDSHIP
Businesses are acting to ensure responsible use of artificial intelligence (AI).

64% Boost AI security with validation, monitoring, and verification.

61% Create transparent, explainable, and provable AI models.

55% Create systems that are ethical, understandable, and legal.

52% Improve governance with AI operating models and processes.

47% Test for bias in data, models, and human use of algorithms.

Source: PwC, 2019 AI Predictions

BASEL GAUGES CYBER RESILIENCE

International standards-setter reviews cybersecurity practices.

A Basel Committee on Banking Supervision report compares bank, regulatory, and supervisory cyber resilience practices across the committee's member jurisdictions. Cyber-resilience: Range of Practices draws from analysis of authorities' responses to previous surveys and exchanges between international experts. The report aims to help banks and supervisors "navigate the regulatory environment" and identify "areas where further policy work by the committee may be warranted."

The Basel Committee classifies its review of cyber resilience along four main categories: governance and culture, cyber risk assessment and management, communication, and interconnections with third-party service providers. Within these areas, the research summarizes current challenges and initiatives along 10 key findings, illustrated by case studies.

Among its findings, the committee reports that most supervisors leverage existing standards for their cyber resilience efforts, including the International Organization for Standardization's ISO 27000 and the U.S. National Institute of Standards and Technology Cybersecurity Framework. And while the report notes supervisory practices converge in areas such as governance and testing, technical

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

IMAGES: TOP, KIDA / SHUTTERSTOCK.COM; LEFT, HAKINMHAN / SHUTTERSTOCK.COM

specifications and cybersecurity expertise differ across jurisdictions.

The report also found high levels of maturity within IT and operational risk management practices, pointing out that banks leverage these practices to address cyber risk and supervise cyber resilience. In particular, the report notes, "Jurisdictions expect banks to have a strategy and framework to comprehensively map and actively manage their IT system architecture." Still, the report finds that banks generally do not have a board-approved strategy that clearly defines cyber risk appetite and tolerance. **– D. SALIERNO**

FEAR THE DIGITAL COMPETITORS

Digital uncertainty heads executives' top 2019 risks.

Nimble, "born digital" companies are coming after their business—that's the top risk keeping business leaders up at night. And they are concerned their organizations aren't ready to compete, according to Executive Perspectives on Top Risks 2019. The report from North Carolina State University's ERM Initiative and Protiviti is based on a survey of more than 800 board members, CEOs, and senior executives.

Specifically, respondents worry their organizations can't adjust their existing infrastructure and operations to meet performance expectations, the report notes. That concern is multifaceted, comprising uncertainty about the organization's digital readiness, ability to keep pace with changing market realities, and lack of innovative thinking about its business model.

Meanwhile, new competitors are scaling up digital business models and "redefining" the customer experience so quickly that established organizations don't see it coming. Such disruptive competition could spell doom for organizations that can't adjust their business models and core operations, warns Jim DeLoach, a managing director at Protiviti.

"Strategic error in the digital economy can result in the ultimate price, if a company continues to play a losing hand in the marketplace," he says. **– T. MCCOLLUM**

MAKING CRIME PAY

Hackers need little money to cost victims millions.

Criminals responsible for companies losing millions of dollars in coordinated cyber attacks are making the most of a small investment. For as little as $34 a month, a criminal business could return up to $25,000. A monthly operating investment of $3,800 could yield up to $1 million per month, according to Deloitte's threat study, Black Market Ecosystem: Estimating the Cost of "Pwnership." *Pwnership* is gaming community slang that describes the act of dominating or defeating an opponent impressively.

The study points out that almost every criminal enterprise uses multiple related, but discreet, tools and services purchased on the black market. It identifies the most commonly

55%

OF FINANCIAL SERVICE PROFESSIONALS CITE GEOPOLITICAL RISK in areas such as China, the Middle East, and emerging markets as a top industry risk for 2019.

49%

IDENTIFY BREXIT AS A TOP RISK.

"It is critical that firms continue to remain vigilant to anticipate and prepare for not only these emerging risks, but the potential cascading effects that may arise from an increasingly interconnected financial system," says Michael Leibrock, chief systemic risk officer for the Depository Trust & Clearing Corp. (DTCC).

Source: DTCC, 2019 Systemic Risk Barometer Survey

IMAGES: TOP, HIBRIDA / SHUTTERSTOCK.COM; RIGHT, MINISTOCKER / SHUTTERSTOCK.COM

used tools and services, their average estimated costs, the tools required to operate real-world criminal businesses, and the estimated operating costs of various cybercrime businesses.

Keith Brogan, managing director with Deloitte, says it is important "to review and compare these criminal businesses to help identify which exploits are the most affordable and lucrative for them to pursue."

When Deloitte modeled enterprise operations for comparison, it found that the most affordable approach is phishing kits, while a campaign that uses several types of malware is the most expensive. It determined this by looking at the most common services, tools, and enablers independently, and calculating the average cost in each category. Researchers then identified which are necessary to perform common malicious activities to establish how the tools and services are related to one another.

Rather than focusing on taking down specific tools, organizations are better off detecting certain types of behavior, the report asserts. To challenge the criminal's cost-benefit scenario, organizations can monitor activities and alter security controls based on tactics, techniques, and procedures—gleaned from threat intelligence—that require criminals to reinvent their operations from scratch. **—S. STEFFEE**

HIGH EXPECTATIONS

Audit committees need internal audit to help them navigate disruptive risks, says National Association of Corporate Directors President and CEO Peter Gleason.

What do audit committees expect of internal audit in 2019? Given the current political and economic uncertainty, progressive audit committees will have their internal audit teams probe the effectiveness of management's scenario planning and operating assumptions that underpin corporate strategy. In particular, they would like internal audit to test the effectiveness of controls and processes related to the management of political risk.

Recognizing the significant investments made in shoring up corporate defenses, audit committees would like to get better assurances that cybersecurity programs are effectively designed and implemented and whether appropriate controls are in place. Similarly, they will expect internal audit to more thoroughly examine the effectiveness of data privacy programs in light of increased compliance requirements and reputational risk. Technology governance is rapidly becoming a major mandate for boards, who will turn to internal audit to better understand risks associated with emerging technologies.

Internal audit possesses a distinct view and perspective on a range of risks that are strategic to the company, and must find opportunities to contribute to board-level dialogue about disruptive risks that are likely to plague the company over the next one to two years.

THE MONEY MULES

Criminals are recruiting individuals to launder stolen funds.

A recent money-laundering sting by European police authorities has drawn attention to the use of "money mules" to hide the origin of stolen funds. The three-month enforcement action resulted in 168 arrests and the identification of more than 1,500 individuals allegedly involved in transferring funds between accounts, Europol reports.

Criminal organizations recruit money mules to move money through the individuals' bank or payment accounts on their behalf. Europol says these individuals often are young, new to a country, and unemployed or in financial distress.

Indeed, last year there was a 26 percent increase in the number of individuals under 21 acting as money mules, according to U.K. fraud prevention service Cifas. "Criminals are more and more turning to social media to recruit new accomplices," through fake-job and get-rich-quick posts, Europol states.

Cybercrime is the source of more than 90 percent of money mule transactions, Europol notes. **—T. MCCOLLUM**

PHOTO: LEFT, WAVEBREAKMEDIA / SHUTTERSTOCK.COM

Back to Basics

BY SCOTT FELTNER   EDITED BY JAMES ROTH + WADE CASSELS

OPENING AND CLOSING MEETINGS

Successful audits start and end with well-planned meetings.

Imagine attending an opening meeting for a scheduled audit. The audit topic is somewhat controversial and there has been pushback on the review's timing. The auditor-in-charge worked hard to find time to get everyone to attend (8-10 people). The meeting is held in a huge conference room, so people are waving across the room and jokingly asking, "How's the weather over there?" There is anticipation mixed with nervousness and anxiety as the auditors introduce themselves. The auditor-in-charge turns on the projector and forwards through the 12 slides in the opening meeting slide deck in about five minutes. She asks if there are any questions (there are none) and thanks them for their time. The group proceeds to exit the conference room feeling deflated. Everyone thinks, "What was the point of that?"

Now imagine attending a closing meeting for a different audit that went well. The clients are engaged with the issues internal audit finds and want to use the audit to help drive improvements in their business. The meeting is held in a huge training room set up with circular tables suitable for 36 people. The auditor-in-charge had difficulty aligning everyone's schedules, so the meeting is held at 4 p.m. on Friday. Six of the 18 people call in to attend the meeting while the rest sit at the back of the room. Unfortunately, the auditor-in-charge shows up just five minutes before the meeting starts and has multiple issues with the technology—he neglects to bring an adapter for the laptop and doesn't know how to use the projector. As a result, the meeting starts 15 minutes late. Two slides in, the meeting is derailed by someone on the phone asking a question, resulting in a five-minute side conversation between the auditor-in-charge and the person on the phone as the others disengage into side conversations or checking their phones and laptops.

Many times, internal audit takes opening and closing meetings for granted and just goes through the motions to conduct them. The difference between meetings that are successful and meetings that are not is preparation and clear objectives. Internal auditors can follow guidelines that will ensure these meetings are informative and engage their audit clients.

Prepare for the Meeting

The meeting room should be visited the day before the meeting to make sure it is appropriate for the number of people attending and that the auditor running the meeting understands how to use the technology in the room. If the auditor-in-charge is uncomfortable speaking in front of people, he or she should rehearse the entire meeting.

SEND BACK TO BASICS ARTICLE IDEAS to James Roth at jamesroth@audittrends.com

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

CONDUCTING EFFECTIVE MEETINGS

Because the opening meeting can set the tone for the audit and the closing meeting is a crucial last step in the audit process, internal auditors can benefit from tips to run the meetings in the most professional manner possible.

- **Consider your appearance at the meetings.** Because internal audit is positioning itself as a competent team of professionals, they should look the part and dress appropriately.
- **Never sit opposite the clients in an "us vs. them" setup.** The audit team should mingle to make the meeting more collaborative.
- **Don't use "auditee" or other internal audit jargon with clients or other meeting participants.** The only people who use those words are auditors.
- **Never read directly from the slides or the audit report.** Points should be made as if the auditor is having a conversation. Use the slide deck and audit report as a guide, not a crutch. If an auditor is unable to do that, then he or she has not prepared well enough for the meeting.
- **Remarks should be addressed to the most senior (nonaudit) person in the room.** This is simply good etiquette.
- **Be culturally sensitive.** In the U.S., staff members present their own findings as a development opportunity. In other countries, the senior member of the audit team is expected to do so. There may be some other cultural etiquette for meetings, as well. Internal auditors should always research cultural norms if they are presenting in another country.
- **The auditor-in-charge should stand up during the meeting, if appropriate.** Standing reinforces that he or she is facilitating the discussion.

Make Your Objective Clear A meeting must have a specific and defined purpose. Before sending that calendar invitation, ask yourself: What do I want to accomplish? This should be shared ahead of time with the client.

Consider Who Is Invited Think about who really needs to be in the meeting. When people feel that what's being discussed isn't relevant to them, or that they lack the skills or expertise to be of assistance, they'll view their attendance as a waste of time. If there are any doubts about certain attendees, make them optional and let them decide whether to attend.

Stick to the Schedule Create an agenda (or slide deck, in this case) that lays out everything that will be covered in the meeting, along with a timeline that allots a certain number of minutes to each item, and email it to people in advance.

Be Assertive If one person is monopolizing the conversation—the fastest way to derail a meeting—call him or her out delicately. For example, "We appreciate your contributions, but let's get some input from others." Establishing ground rules early on will create a framework for how the group functions. Internal audit is in charge of the meeting. Discussions of risk ratings, for example, can be a derailer that the auditor should consider discussing outside of the meeting.

Start on Time, End on Time Knowing that time is valuable, do not schedule any meeting for more than an hour. Sixty minutes is generally the longest time people can remain truly engaged. A *Harvard Business Review* article, "The 50-minute Meeting," suggests allowing 10 minutes of the 60 minutes for travel and administrative time. And if only 30 minutes is needed, don't schedule an hour.

Ban Technology Laptops and smartphones distract people from being focused on the meeting or contributing to it. Instead, they'll be sending emails or surfing the web.

Note Action Items and Follow-up So that everyone is on the same page, a follow-up email highlighting what was accomplished should be sent within 24 hours to all who attended. Document the responsibilities given, tasks delegated, and any assigned deadlines.

If opening and closing meetings seem repetitive and boring, consider the actors who perform in some Broadway plays for years. They strive to do every performance, even the 873rd, with the same passion as the first. They polish and perfect it each time. Clients deserve the best from internal auditors, and there will always be someone in the room who hasn't seen the slide deck or been through an audit before. The right preparation can make these meetings valuable and productive for auditor and client. Ia

SCOTT FELTNER, CIA, CISA, *is vice president, internal audit, at Kohler Co. in Kohler, Wisc.*

BY PAUL SLYE + CHRIS WELTER EDITED BY STEVE MAR

TRUSTED FOR TECHNOLOGY

Nordstrom's IT audit specialists pinpointed five areas to prove their worth as advisors.

Technology is a key enabler of business value. Internal auditors must be able to verify that these processes provide the intended return on investment and that technology risk decisions and resources are optimized. Without the necessary skills, auditors may not deliver the value that the business expects of them.

Most technology auditors at Nordstrom are integrated auditors—technologists with business degrees and years of consulting firm experience. They work as peers to three other unofficial designations of auditors: operations, business intelligence, and compliance.

Nordstrom uses two metrics to determine whether its technology auditors are trusted advisors: whether clients return to request internal audit's services and whether the audit recommendations result in business value. To provide valuable counsel, technology auditors need to understand the emerging technologies with which their business partners are working as well as developments such as DevOps, the Internet of Things, and serverless architecture. In learning to provide such advice, technology auditors focused on five areas.

Cybersecurity and Privacy

Most industries consider cybersecurity and privacy to be inherently high risks. As a company that relies on technology, Nordstrom has hired professionals with cybersecurity certifications to consult and audit how to optimize its risk posture.

In turn, technology auditors have interpreted and applied controls from security frameworks to Nordstrom's new, cloud-based environment. Two frameworks auditors use are the International Organization for Standardization's ISO 27002—Information Technology–Security Techniques–Code of Practice for Information Security Controls and the U.S. National Institute of Standards and Technology Cybersecurity Framework.

Auditors translate the security requirements of these frameworks into the language the audit clients use. For example, application teams have adopted a DevOps structure whereby any member of the team can make changes to production code. Auditors explained to the team the potential for unauthorized code change and the requirements contained in the security standards. That helped team members realize they should implement logging and file-integrity monitoring linked to change tickets as a compensating control to ensure that unauthorized changes would be detected immediately. As teams learn about security risk and controls, they make more risk-optimized decisions.

Technology Governance

Nordstrom's internal auditors rely on ISACA's COBIT 5

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

TO COMMENT on this article, EMAIL the authors at paul.slye@theiia.org

framework to evaluate technology governance maturity on a repeatable basis. Auditors merged COBIT 5 and ISO standards to create a framework specific to Nordstrom as a basis for audits. This framework enables auditors and audit clients to see where their activities fit into the big picture.

Having a framework has enabled the department to partner operational auditors with technology auditors to perform integrated audits on nontechnical aspects of technology governance. In one review, auditors provided assurance that technology projects were delivering the value promised in the business case. The auditors on the integrated audit expanded their knowledge by covering tech strategy, enterprise architecture, and performance measurement.

Data Science

Nordstrom's auditors have written more compelling audit reports by testing 100 percent of populations using data science techniques. To write such reports, all auditors are expected to have basic knowledge of Microsoft Excel, statistics, and data validation. Internal audit leverages data extraction tools to obtain data for use in creating impactful issue statements in reports.

Data science tools are especially useful when joining two or more data sets (see "Beneath the Data" on page 42). In one project, internal audit extracted incident ticket information and linked it with information about problem tickets, root-cause analysis, and application IDs from multiple systems of record. To extract knowledge from these unique data sets, auditors used data visualization tools to tell the story of how well the company's change-management controls were performing and if it was learning from the incidents. The client capitalized on the analysis to track how much progress was made since the report was delivered.

> **Business partners now expect audit findings to be supported by data.**

Robotic Process Automation

A recent development for Nordstrom's internal auditors is the use of robotic process automation (RPA). Projects are advisory in nature and aligned with internal audit's goal of identifying ways to reduce expense or work effort. Partnering with the company's restaurant and tax divisions, auditors created robots to automate manual processes relevant to food and beverage licensing and entry of invoices. Through this automation, auditors reduced the clients' payroll expenses.

Another example is the company's user-access review and validation process. Auditors incorporated control owners' control documentation into internal audit's testing procedures and used RPA to test attributes. One test validated that users had their access revoked timely. RPA has enabled auditors to accomplish more testing within the same time frame.

Communication

Nordstrom's technology auditors have focused on improving their verbal and written communication skills. To communicate effectively with the technology organization, the department's IT audit director spent six months working directly for technology leaders before starting his role in internal audit. During this time, he learned those executives' leadership and communication styles, which internal auditors now incorporate into their reports to increase their impact.

Auditors also have become persuasive communicators, effective negotiators, and great listeners. They have increased stakeholder buy-in by using data to buttress audit findings and action plans. Business partners now expect audit findings to be supported by data, even when the topic is difficult to quantify.

However, visualizing data is not required for all audit reports. Sometimes, visualizations cause the client to jump to assumptions without reading all the details. Some clients prefer to read the text instead. While audit reports should always focus on the most important risks and opportunities, auditors tailor the department's report style to meet stakeholders' desired format.

Earning Trust

To benefit the organization, internal audit needs to constantly develop staff members into trusted advisors and retain them. So far, Nordstrom's efforts have:

- Increased risk-focused conversations led by leadership, resulting in more effective controls.
- Led to a cultural shift to spend time building technology risk mitigation strategies.

In the process, technology auditors have received high client satisfaction ratings as well as more requests from management to perform work. Moreover, management is more proactive in driving change about issues that auditors have identified, even before they receive audit reports. Once clients realize that an audit report can propel them faster toward achieving their objectives, they tend to become repeat clients and tell their peers throughout the organization. Ia

PAUL SLYE, CISSP, CISA, *is an internal audit manager at Nordstrom in Seattle.*
CHRIS WELTER, CISA, *is an audit principal II at Nordstrom.*

BY LYNN FOUNTAIN EDITED BY CHARLIE WRIGHT

INTERNAL AUDIT'S EVOLVING CYBERSECURITY ROLE

Auditors need to become involved in helping their organizations address cyber risks.

Technology is progressing at such lightning speed that even IT specialists struggle to keep their fingers on the pulse of technological change. So how are internal auditors expected to adequately assess and examine the various risks emerging in this cyber age?

As technology continues to advance, internal auditing must evolve. For many years, internal audit departments relied on IT audit specialists as partners in integrated audits. Although those specialists focused on systems and technology, integrated audits worked best when operational and financial auditors knew what to look at from an IT perspective.

In today's world, internal auditors cannot delegate responsibility to their IT departments or IT auditors. All auditors should have a solid understanding and awareness of more than just general and application controls. They should realize the technology risks and their potential impact.

One of the most prevalent issues organizations face today is the constant threat of cyberattacks. Every day there is some new threat, breach, or cybersecurity incident. It is now imperative that all internal auditors understand the underlying drivers as well as the nature and causes of cyber risks. With this knowledge, internal auditors can add significant value to the organization by assessing and helping management strengthen cybersecurity.

Knowledge Is Power

Yes, internal auditors know how to use a computer and a cell phone, but do they realize the risks these technologies pose? What you don't know can hurt you! In today's business environment, training on cybersecurity issues should be a basic curriculum expected of internal auditors. Training that is essential for internal auditors includes understanding:

- The threat of cyber fraud to their organizations and the manner in which it could present itself.
- Procedures that should be followed to assess cyber risk.
- Types of new and existing breaches.
- Various tools for managing cybersecurity issues.
- Methods to prioritize assets at risk for protection plans.
- Methods to appropriately allocate resources to protect assets.

Understand Cyber Risk Frameworks

Organizations need to understand and use a structured cyber risk framework to mitigate threats. Although there are several frameworks, some organizations may focus on a specific framework, depending on their industry.

One of the most widely used frameworks is the U.S. National Institute of Standards and Technology's

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

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

(NIST's) Cybersecurity Framework. The framework directs organizations to use a standard protocol in their cybersecurity efforts to identify and protect assets, and respond to and recover from incidents.

Identify and Protect Assets at Risk

The NIST framework recommends that organizations identify assets within the organization that are most susceptible to cyber threat. Next, it advises organizations to prioritize assets for protection, and develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

Identifying and protecting assets is similar to other risk assessment processes and is an area in which internal auditors can provide valuable insight to help protect their organizations. Auditors can help their organization by:

- Following a structured approach to perform a top-down assessment.
- Evaluating cyber risks within individual audits.
- Assessing the organization's capabilities to manage assets that might be impacted by a cyber risk event.
- Evaluating whether management and the board have developed a comprehensive cybersecurity strategy.
- Fully integrating cyber risks into the annual audit plan.
- Determining whether management is using the most effective process to prioritize assets for protection and allocate resources.

Monitor Detection Procedures

Detecting cyber threats is the third component the NIST framework recommends. Once assets have been identified and protected, the organization should develop and implement appropriate activities to take action when a cybersecurity event is detected.

As with The Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control–Integrated Framework* monitoring component, performing detection procedures is management's responsibility. However, internal auditors can test detection procedures to ensure they are designed appropriately.

Management should follow a well-devised protocol to develop, design, and implement detection procedures. Auditors can review and test that protocol and ensure detection procedures are addressing the most vulnerable assets. This act requires auditors to collaborate with management to fully understand the procedures used in the design phase and in identifying which assets are prioritized as higher risk.

Respond to Incidents

This component of the NIST framework includes activities to undertake when the organization has detected a cybersecurity incident. The objective is to contain the incident's impact on the organization.

Compare a cybersecurity incident to a fire. Both are "all hands on deck" events. If management has not structured a cyber risk program appropriately, there may be many reactive actions and ad-hoc approaches to plugging the gaps. Internal auditors can be important consultants in this situation.

Often when a breach occurs, management looks for the quick fix. This may not always be the best solution. The response must consider not just the tactical steps taken to fix the problem but all of the ancillary communication and documentation that is required. In this circumstance, internal auditors can provide an independent perspective and guide management on the best path to follow to respond to the incident. But to be helpful, auditors must understand the technology issues as well as the incident-response processes.

Use Recovery to Learn Lessons

Recovering from a cybersecurity incident is comparable to recovering from an illness. When a person discovers he or she has a serious illness, all focus is placed on acting to respond to the illness. At that point, the mindset is survival rather than recovery.

As defined by NIST, the recovery phase occurs after the organization has responded to a breach. This phase includes identifying activities to maintain plans for resilience and to restore any services that were impaired due to a cybersecurity incident. The organization must be able to constructively review what occurred and extract appropriate lessons learned from the incident. Then the organization must incorporate those lessons into its current response protocol.

By assessing the lessons learned from an incident, internal audit can contribute to the ongoing viability of the organization's cybersecurity incident plan. This assessment can assist the organization in evaluating gaps in how assets were identified and prioritized, how protection procedures were prioritized and executed, how detection procedures were implemented, and how response procedures were put into effect.

Internal Audit's Expertise

The NIST Cybersecurity Framework's guidance is just a sample of important concepts to understand. As technology evolves, so do the duties of internal auditors. The profession needs to step out of its comfort zone and insert its expertise into addressing cyber risk. Ia

LYNN FOUNTAIN, CRMA, CPA, CGMA, *is an internal control, risk management, and business process consultant in Overland Park, Kan.*

Fraud Findings

BY GRANT WAHLSTROM + ANISA CHOWDHURY EDITED BY BRYANT RICHARDS

THE PHONY CUSTOMER FRAUD

An unscrupulous employee reaps the benefits of weak internal controls.

Brightstar Corp. is a solar panel company with an annual revenue of $4.5 billion. It had recently acquired Solarstar Inc., a smaller competitor. Both companies employ commission-only sales representatives; however, commission plans vary between the companies. Brightstar pays sales representatives upon the installation of a solar panel system, while Solarstar's commission plan pays half a commission upon the signing of a customer contract. The remaining commission is paid after installation of the system. If the customer cancels the installation, the commission already paid is clawed back against future commissions.

Robert Schull and Alysa Cayden, Brightstar's forensic audit team, were conducting a training session with the recently hired director of compensation, Lisa Myers, on fraud schemes perpetrated by sales representatives. At the end of the presentation, Myers approached Schull and Cayden to discuss her concerns about Eddie Fogbottom, a sales representative in the Austin, Texas, market.

Fogbottom was a rising superstar at Solarstar. Before joining the company, he was an executive in loss prevention at several large publicly traded companies. He had incredible success as a sales representative and was recently promoted into a highly sought-after manager role within the company's national sales team. Shortly after accepting his new position, 39 of Fogbottom's sales were cancelled, representing $10,000 in commissions that would need to be clawed back. Because it was such a large amount, Myers contacted him to discuss a repayment plan.

Fogbottom told Myers that the company could not claw back the commissions. When he was promoted, he had a clause written into his offer letter allowing him to keep all commissions for prior sales, even if customers cancelled their accounts. Myers suspected fraud.

Solarstar uses electronic contracts, which are emailed to the customer when completed. The customer reviews the contract, and electronically signs and returns it. Contracts are not legally binding until the contract is returned and a down payment is received. An electronic time and date stamp is recorded on the contract as well as the customer's computer internet protocol (IP) address.

Schull and Cayden began reviewing the cancelled contracts. The team identified several days where Fogbottom sold products to multiple customers in what appeared to be strip malls in the Austin market. What caught the attention of Schull and Cayden was the fact that the contracts were signed and returned within several minutes of each

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

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

other. Even more perplexing, the contracts were returned from the same IP address.

The team began conducting customer service calls to the alleged customers to determine why they cancelled their purchases. Surprisingly, none of the phone numbers documented on the contracts were in service. In addition, an internet review of the customers revealed that not a single customer had an internet presence.

The investigation team turned their attention to the down payments received on the contracts. Solarstar required its sales representatives to collect a down payment when a customer signed a contract. The sales representative would document the collection in the company's order system. If the down payment was paid with a check, the sales representative would bring the check into the local sales office to be compiled and sent to the company's lockbox. A review of the order system revealed that Fogbottom documented that checks were obtained during the contracting process, but none of them had been received in the lockbox.

Cayden reviewed the customer sites using Google Earth. The review revealed that many of the customer locations did not appear to exist or had been constructed after Google's last update. Schull enlisted the assistance of Brightstar's area general manager, Michael Gonzalez. A 25-year Brightstar veteran and lifelong resident of Austin, Gonzalez accompanied Schull to the customer locations. It came as no surprise when Schull and Gonzalez found themselves standing in empty fields. Schull documented the visits with photos of the alleged customer sites.

Schull then reviewed Fogbottom's employment history. An internet search revealed that Fogbottom had, in fact, worked for the organizations he had listed on his résumé. However, no references were listed in his employment file. Schull was suspicious about why a former loss prevention executive would accept an entry-level sales position.

Fogbottom was asked to come to the Austin office for an interview with Schull and Karol Vesey from human resources. Schull believed the interview would be challenging as Fogbottom had extensive interviewing experience in his loss prevention role. During the initial stages of the interview, Fogbottom presented himself as a professional loss prevention executive turned successful national sales manager. He bragged about his experience and connections to the community.

LESSONS LEARNED

- » A combination of fundamental internal control activities helps minimize fraud.
- » Conduct and update a fraud risk assessment regularly. In this case, a fraud risk assessment should have identified the control weakness in the backlog report, commission payment process, and revenue reconciliation process.
- » Conduct appropriate background checks on key employees to identify any red flags for possible unethical behavior.
- » Perform regular reviews of installation backlog reports to identify irregular activities. Detecting any potential exploitation is the best approach to minimizing negative unintended consequences.
- » Conduct monthly reconciliations of revenue collections. Discrepancies should be researched immediately and escalated if unresolved.

When presented with the photographs of the empty fields, Fogbottom's demeanor changed. He alleged that a general contractor named Sal was constructing all three strip malls, and that the customers met him at a local coffee shop where they all completed their contracts in succession. Fogbottom could not remember Sal's last name or produce a contact number for him or any of the alleged customers. Initially, Fogbottom refused to admit that he falsified the contracts in question. However, after an extensive interview, Fogbottom admitted that he was having personal problems and was fired from his former employer. He also admitted that he falsified the contracts for the commissions because he had taken a substantial pay cut from his previous role and was having trouble making ends meet.

Fogbottom could not remember Sal's last name or produce a contact number.

Fogbottom was terminated, but no charges were brought, and the money was clawed back. Solarstar updated its commission plans to only pay sales representatives upon installation. Two weeks after Fogbottom's termination, Schull received a call from Brightstar's Fresno, Calif., office where the same fraud scheme was suspected and later validated. Ia

GRANT WAHLSTROM, CIA, CPA, CFE, *is the forensic audit manager at a security company in South Florida.*

ANISA CHOWDHURY, CPA, *is a senior forensic auditor at a security company in South Florida.*

Ten years ago, amidst unprecedented economic upheaval, RICHARD CHAMBERS became The IIA's president and CEO. The internal audit profession has changed much since then, he says, and it will need to continue to evolve.

Trials *and* Transformation

Anne Millage

Photograph by Doug Scaletta

Richard Chambers became the ninth president of The IIA in January 2009 during the onset of the global economic crisis. It was a time when companies were experiencing a major loss in shareholder confidence due to colossal risk management failures and a lack of corporate accountability. These dark times revealed vast new opportunities for internal audit to help protect organizations and enhance their performance.

Chambers says internal auditors grasped those opportunities by pivoting swiftly to focus on the emerging risks brought on by the financial crisis and the impact these risks were having on their organizations. The profession became much more risk-centric in those early years of the prolonged financial downturn. The result? Internal

audit solidified the stature that it had earned in the prior decade and became a critical component of the systems of risk management and internal controls in modern organizations. “The past decade has been about proving that the confidence that was conveyed to us in the early 2000s was deserved,” Chambers says. “This decade, I think we’ve earned that trust even more.”

On the eve of Chambers’ 10th anniversary with The IIA, we sat down to discuss how the internal audit profession was impacted by the financial crisis, how it responded, and how it has evolved.

INTERNAL AUDITOR You became The IIA’s CEO during the greatest economic upheaval since the Great Depression. How was that crisis impacting internal audit?

■ ■ **RICHARD CHAMBERS** Having been in this profession over 30 years at that point—whether it was my time in government or in the corporate sector—my experience had been that whenever organizations’ resources were severely impacted, it would translate into an even more drastic impact on internal audit. Historically, I had witnessed internal audit departments being divested at a much higher rate than the organization as a whole as executives sought to trim costs.

I was anticipating that scenario at the end of 2008, but I was pleasantly surprised as the next couple of years unfolded and internal audit was not disproportionately downsized in most organizations. In fact, reductions in the profession at that time were similar to what organizations were experiencing overall as a result of the financial crisis.

Why was it different this time?

■ ■ Internal audit’s resilience appeared to be a reflection of the stature the profession had gained in the previous decade. One difference between this recession and the recession of the early 2000s and those that came before, was there had been a sea change in internal audit’s positioning within the governance structure. Following the financial reporting scandals of the early 2000s that involved Enron, WorldCom, and others, we saw legislation and regulations implemented that fostered a stronger emphasis on controls—particularly financial reporting controls. As a result, internal audit was ushered from the back room to the boardroom where it developed a stronger relationship with the audit committee.

Was internal auditing being redefined?

■ ■ We didn’t redefine ourselves; we started living our definition. In the early 2000s, internal audit became much more risk-centric. If you think about it, there was not even a standard that required internal audit to do a risk assessment as part of its audit planning process until 2002. So, we had only a short time between the onset of the standards mandating a risk assessment and the beginning of the financial crisis to get a full appreciation of what being risk-centric meant.

With the onset of the financial crisis in 2008, suddenly there were countless new risks facing our organizations. The crisis had exposed the ineffectiveness of risk management, itself, as a critical risk. There was a notable spike in operational risks as companies were compelled to achieve greater operational efficiency and effectiveness. And almost half of chief audit executives (CAEs) reported increased coverage in cost reduction and containment in 2008 and 2009. We started to see risks around technology, cybersecurity, culture, social media, and so on. And compliance risks became critical—particularly as we saw legislative provisions such as those in the U.S. Dodd-Frank Wall Street Reform and Consumer Protection Act make their way into regulation.

So in the wake of the financial crisis, there was a radical and rapid rebalancing of internal audit’s focus. It reprioritized and emphasized a broader portfolio of risks. Internal audit was living up to its definition of being risk-based.

Was internal audit’s response to the financial crisis appropriate?

■ ■ It’s hard to argue with the success internal audit achieved at the time. It was an unprecedented time for the profession. While we were busy rolling up our sleeves to help our organizations respond to the emerging financial crisis-related risks, there were already those asking, “Where were the internal auditors, and why weren’t they looking at risk management in financial services organizations?” And my answer was, there wasn’t a lot of emphasis by internal audit on the effectiveness of risk management before 2008 because we were being asked to fight the last war by focusing on internal controls over financial reporting. Very few people were focused on the effectiveness of risk management in financial services—including those management and board members who were actually responsible for risk management. The emphasis was to ensure there were no more Enrons and WorldComs. When you’re busy looking behind, you miss what lies ahead.

Are there areas in which the internal audit profession has fallen short?

■ ■ As a profession, we’re still not demonstrating some of the attributes of great professions. For example, I don’t see

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

the level of conformance to the *International Standards for the Professional Practice of Internal Auditing* that we should be witnessing. I chaired the Internal Audit Standards Board in 2002 when we adopted the first standards that required external quality assessments. If you told me in 2002 that I'd be sitting here in 2019 saying that we still have such limited conformance, I would not have believed it.

When I say there's nonconformance, I don't mean to imply that no one is paying attention to the *Standards*. I'm talking about conformance with the full set of *Standards*. There is definitely widespread adherence to parts of the *Standards* around the world. There's a much higher degree of conformance in large, publicly traded companies in North America and Europe than in other types of companies or organizations in other markets. But is conformance where it should be? Absolutely not.

Additionally, I would have thought there would be greater recognition of our *Standards* around the world. The IIA's *Standards* are widely acknowledged within the profession, but they're not necessarily widely recognized by others, such as regulatory bodies, relying on internal audit's work. I continually deliver this message to global regulatory bodies: "There is only one set of global internal audit standards in the world. Why aren't you promoting them?"

> If we don't help our organizations anticipate risks that may lie beyond the line of sight, we're likely to be ill-prepared to help them when those risks materialize.

Are there other areas in which internal audit could improve?

I'm concerned that the profession is not as assertive as it should be in speaking out. There's a certain comfort level that says, "Nobody is pushing me to do this; therefore, I'm going to stay the course." And when you take that approach, you leave your organization vulnerable to value-destructive calamities or scandals. For example, internal auditors are reluctant to tackle sensitive topics such as corporate culture, executive compensation, or management of risks associated with sexual harassment policies in their organizations. As a result, these are risks that seem to routinely get companies in trouble.

Too often, a courage deficit exists. Internal audit has to be courageous enough to address issues such as these that are not popular. We have to be courageous enough to speak the truth even when someone isn't interested in hearing it. And we have to be courageous enough to speak truth to power. If a CEO is engaged in questionable activities, or fraud, the CAE must summon the courage to alert the audit committee.

Are there other reasons internal auditors fail to speak up?

Internal audit is still reluctant, in some instances, to take on risks that are outside of its comfort zone. For example, culture, cybersecurity, and blockchain technology are areas in which internal audit may not have a lot of expertise, so they are frequently neglected despite the risks they present to the organization. Internal audit's mandate is to be risk-centric, not just risk-centric in the risks with which we're comfortable.

Internal audit also has not made the kind of progress that organizations need in identifying emerging risks. We are still inclined to see the risks that lie immediately in front of us. If we don't help our organizations anticipate risks that may lie beyond the line of sight, we're likely to be ill-prepared to help them when those risks materialize.

You've talked a lot about expectation gaps with stakeholders over the years. Why does internal audit struggle to narrow those gaps?

Throughout my career, I've witnessed how dynamic stakeholder expectations can be and how quickly they can pivot. In the early 2000s, there were some who thought internal audit needed to be consultants in their organizations—out there helping people better understand their own risks and problems.

Then came tbe U.S. Sarbanes-Oxley Act of 2002. And regulatory compliance risks associated with financial reporting controls rapidly became the priority of internal audit's stakeholders. By 2005, according to a PwC survey that I led, 71 percent of internal auditors at publicly traded U.S. companies reported they were spending more than half of their time on Sarbanes-Oxley compliance. With the onset of the financial crisis in 2008, the risks that companies faced and internal audit stakeholder expectations changed quickly. Internal audit realigned its coverage to address new risks. By

PULLING TOGETHER

Recessions and swift economic downturns are very challenging for professional associations. As Richard Chambers puts it, "If other sectors catch a cold during a recession, not-for-profits catch the flu." The impact of the 2008 financial crisis on The IIA was great. "One of the first things that companies cut if the economy turns very soft is training and travel dollars," Chambers explains, "so the impact was swift and severe."

Chambers says he knew when he became president and CEO in January 2009 that the financial challenges were going to necessitate downsizing to a leaner, re-engineered Global Headquarters. He and the Global Board of Directors had to make some difficult calls. "We didn't really have a lot of choices," he recalls.

Navigating through the crisis required full involvement – from the Board, volunteers, and IIA staff. "Those early months of 2009 were really spent working collaboratively," Chambers says. "One of the greatest achievements of The IIA in the past 10 years was those first few months when the staff came together." The Institute put together action teams to look at opportunities to cut costs and to grow revenue. "It was a collaborative process that really exemplified the very best of who we are," Chambers says. The board was "absolutely unwavering" in its support of the steps The IIA took, he adds.

In the ensuing months, The IIA discontinued some initiatives and refocused on serving its members. "We redefined what service meant," Chambers says. "We began to look at the member value proposition."

"Throughout this decade, we've continued to make great progress in serving the members," Chambers adds. Membership continues to grow, and The IIA is poised to crest to 200,000 members worldwide.

The results of the last 10 years have allowed The IIA to make some extraordinary investments that Chambers says will become more evident to members over the next couple of years. "We're making unprecedented investments in technology in support of the profession," he notes.

The IIA takes a strategic view of its role in supporting the organization and in serving its members. Its strategic plans have served as the blueprints for supporting member expectations and meeting the needs of the profession. "The IIA has never been stronger," Chambers says.

JULIE FLETCHER

Chambers says IIA Board support has been integral to The Institute's success over the past decade. Chambers and Board chairs from the past 10 years recently gathered at The IIA's Midyear meetings in Orlando, Fla. From left to right: J. Michael Peppers, Denny Beran, Günther Meggeneder, Phil Tarling, Richard Chambers, Patty Miller, Anton van Wyk, Naohiro Mouri, Larry Harrington, and Paul Sobel. (Not pictured: Angela Witzany and Rod Winters)

2012, according to an IIA survey, the percentage of internal audit plans dedicated to Sarbanes-Oxley compliance had fallen to less than 15 percent while the combined percentage of coverage dedicated to operational and compliance risks surged to more than 40 percent. Stakeholder expectations are changing yet again, 10 years after the financial crisis.

Recent reports suggest that management and boards are looking for internal audit to focus on key risks beyond financial reporting and compliance. As KPMG recently observed, risks related to culture, incentive structures, cybersecurity, data privacy, global supply chain, and outsourcing, as well as environmental, social, and governance risks, can significantly impact share value. It remains to be seen how extensively and rapidly internal auditors will pivot to address these risks. However, I am confident that they will.

The greatest danger of an expectations gap occurs when there is a swift and sudden shift in the risks that an organization faces. There's often a lag time between when a risk becomes critical for an organization and how quickly internal audit can address it. And it's in that window where stakeholder expectations get ahead of internal audit. That's why it is critical in 2019 and beyond for internal auditors to have the agility to change direction swiftly to keep pace with stakeholder expectations.

> Internal audit has a huge obligation in the next decade to embrace the fourth industrial revolution—a new era that extends digital technologies in new and unanticipated ways.

Where do you see internal audit in 10 years?

If, in some respects, in the early 2000s internal audit fell back into the era of hindsight—looking at whether financial controls were appropriately designed and implemented—there's been a much greater emphasis on insight in this last decade.

The decade ahead offers internal audit a great opportunity to continue to build on the way we serve organizations by also providing foresight. Being able to look at emerging risks, to look out further and identify what actions need to be taken, and to talk more about what risks may present themselves if certain actions aren't taken provides tremendous value.

Internal audit also has a huge obligation—and opportunity—in the next decade to embrace the fourth industrial revolution—a new era that extends digital technologies in new and unanticipated ways. We are in an era where the volume and complexity of data dwarfs anything we've seen. It defies imagination in some ways. Internal audit has to recognize not only what that means in terms of the risks our organizations face, but also the approach we take to auditing them.

In the coming decade, artificial intelligence (AI) is going to become much more pervasive. I often get asked whether AI is a threat to the internal audit profession. It's not a threat unless internal audit continues to do the things that we've always done. A lot of the activities that internal audit has historically done are susceptible to being replicated or done through AI. Hindsight is much easier for AI to do, for example, than foresight. As yet, however, AI cannot combine data, information, trends, rumors, breaking news, competitors' actions, and even hallway gossip to formulate reasoned and rational suggestions of future developments and their associated risks and opportunities—foresight. We have the opportunity and the obligation to address AI and similar technological innovations not only from the standpoint of what the risks are to our organizations, but also in terms of how internal audit uses it. AI can be a great contributor to internal auditing. It can help us become more efficient and target our efforts and resources.

So how does the profession continue to grow?

Internal audit is definitely on stronger footing than we were 20 years ago, or even 10 years ago. However, this profession, like all professions, should always be prepared to prove its worth. I don't think we have any guarantees of what lies ahead for internal audit. We are a respected resource right now, and we will stay there as long as we recognize the responsibility that comes with it. Internal audit must always be prepared to lean forward and not rest on its laurels.

ANNE MILLAGE *is editorial director and editor-in chief of* Internal Auditor *magazine.*

Building the Audit Function

A strategic, measured approach to setting up shop can produce lasting results and strong relationships.

Neil Hodge

Illustrations by Edwin Fotheringham

Building an internal audit function from the ground up may seem like a daunting task, but taking a measured approach and prioritizing what should be done first can ease some of the difficulties. Handling these initial steps with care also helps build trust in organizations that may have no experience with internal audit or may be suspicious of its motives. By selecting key areas of focus and seeking to make "quick wins," chief audit executives (CAEs) can soon win over management and the rest of the business, and establish a solid foundation for the audit function.

THE LAY OF THE LAND

Alyssa Martin, partner in charge at risk advisory services firm Weaver in Dallas, is no stranger to setting up internal

audit functions from scratch. She says she typically sets up around three or four functions per year on behalf of clients, and that she has established—or "reconstituted"—more than 20 in her career to date.

Martin says the reason behind the organization's decision to set up an audit function can provide vital clues about what it will look like and how it will be resourced. Potential reasons include regulatory requirements; past governance failures that impacted operations; financial incentives such as improving processes, increasing efficiency, and minimizing potential frauds; or pressure from a large customer to provide it with more assurance. "The different circumstances behind the move to set up an internal audit function can influence the way it is developed, what its scope is, and

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

what budget and resources it will have," she says.

The way in which internal audit will operate also needs adequate consideration, Martin adds. If, for example, the function comprises a head of internal audit who oversees a fully outsourced team, that individual must be a strong leader with lots of experience. He or she must be able to take charge and establish what the function's priorities should be, as well as determine what expertise the organization needs to obtain quickly.

Martin says internal audit needs a "sponsor" within the organization to champion the function and to send a message to the board and the rest of the organization that internal audit is a key player in ensuring effective governance and sound practice. Moreover, CAEs need to liaise and establish good working relationships with key second-line assurance functions in the business, particularly the chief risk and compliance officers, as well as maintain communication with the chief financial officer (CFO). "Internal audit can't act in isolation, and especially not when it is a new department," she says. "It needs to establish key partnerships with other functions in the business to see how they operate, how they view risk, and to learn their approaches."

Martin also notes the importance of building a good relationship with the audit committee, management, and the organization in general, and she stresses the need for audit heads to understand the audit universe and identify which activities are a priority for internal audit's involvement. "Find out where internal audit needs to be active first and what skills and experience you need to have to make a good impression straight away," she says. "You have to choose where you can make an immediate impact first to gain trust with management and the organization."

The head of internal audit also needs to look closely at the budget he or she has been given. "A low budget impacts hiring choices and what you can realistically do," Martin says. "It also means that you have to prioritize areas that need the most work or immediate focus." She advises audit leaders not to complain about receiving less funding than expected, noting that effective use of allotted resources can allow for quick wins and help build confidence with managers who control the purse strings, thereby making them more likely to agree to additional funding later.

OBTAINING BUY-IN

Arif Zaman, head of internal audit at real estate company Emaar Industries and Investments based in Dubai, United Arab Emirates, was formerly a risk advisor at a consulting firm where he helped large corporate clients set up or reconstitute internal audit functions. Zaman says the experience taught him what a "good" internal audit function should look like, and what constitutes best practice.

Having board buy-in from the start is essential to the success of any internal audit function, Zaman says. "Once you have board backing, you can then get approval for the internal audit framework and reporting structure, which will allow internal auditors to maintain their independence and objectivity," he explains.

Like Martin, Zaman says internal audit must know who will champion the audit function—usually the second line of defense functions like compliance or risk management. He adds that, to maintain independence, internal audit should report to the audit committee or directly to the board. Once the reporting line is defined, the head of internal audit should ensure that three documents are drawn up quickly:

- An audit committee charter to define the role and responsibilities of the committee (with board approval).
- An internal audit charter to define the scope, role, responsibilities, and reporting structure of the internal audit function.
- The standard operating procedures, which are policies and procedures that cover the annual audit plan, approval process, engagement plan, audit execution, audit reporting, follow-up, reporting, and quality assurance.

82% of stakeholders say internal audit finds potential revenue enhancement, cost savings, or smarter capital expenditure spending, according to a 2018 KPMG survey.

QUICK CHECKLIST*

Several activities should be considered when establishing an internal audit function:

- Identify key internal and external stakeholders and obtain a clear understanding of their expectations.
- Communicate the role of internal audit to the board, audit committee, executive management, and the rest of the organization.
- Ensure that there is a functional reporting line to the audit committee and – ideally – an administrative reporting line to the CEO.
- Put an internal audit charter in place – one that is approved by the audit committee.
- Conform with The IIA's *International Standards for the Professional Practice of Internal Auditing.*
- Prepare an internal audit strategic plan that considers the organization's objectives and key risks as well as any gaps within its assurance framework.
- Assess the organization's risk maturity to help determine the internal audit strategy and approach.
- Agree with management on an annual internal audit plan that is approved by the audit committee.
- Agree with management on budgets (financial and staffing).
- Coordinate internal audit work with that of other assurance providers (internal and external).

**A version of this checklist originally appeared in the Chartered Institute of Internal Auditors guide, How to Set up a New Internal Audit Activity. Adapted with permission.*

According to Zaman, understanding the business, how it operates, and—crucially—its culture, also are key steps to successfully setting up an internal audit function. "It is very important to be acquainted with the culture and business acumen of the company," he says. "It gives a general idea of the company's risk maturity and its control environment. It also provides useful insight about how an internal auditor should determine his or her approach and how to pitch the internal audit department framework within the organization."

Zaman also notes the importance of considering the culture of the country in which the organization operates. "Internal audit is nothing new in countries like the U.S., U.K., or elsewhere in Europe," he says. "These countries have an understanding and appreciation of what internal audit can provide. But in developing markets, awareness of what internal audit is supposed to do, and what it is capable of, can be quite low."

To help gain trust in the organization, Zaman says it may be best if internal audit has a pragmatic—rather than dogmatic—mindset. He stresses that flexibility may be necessary, as a "by the book" approach may intimidate business units and deter them from coming forward and reporting problems. "You want to establish a culture of openness and transparency that encourages people to come forward with concerns, rather than reinforce the stereotype of

"You have to choose where you can make an immediate impact first to gain trust with management and the organization."

Alyssa Martin

"It is very important to be acquainted with the culture and business acumen of the company."

Arif Zaman

internal audit being an internal policeman," he says.

Zaman also agrees with Martin that achieving quick wins early on can help turn people's attitudes around in the auditors' favor. He warns against starting with sweeping, ambitious objectives such as advising an overhaul of the way the organization is run or recommending controls around every single business process. Instead, Zaman suggests looking at simple ways to help cut costs and increase efficiencies, being sure to quantify the immediate and long-term cost savings. "Concentrate on just doing the main audit work you need to do first and where you know you can succeed," he says.

"Any new internal audit function will live or die by the people it has on its team."

Phil Tarling

If internal audit wants to show it is independent, it needs to assert that independence from the beginning."

Seidu Sumani

REPLACING A PREVIOUS FUNCTION

Seidu Sumani, senior vice president, head of internal audit, at MFS Investment Management previously set up an internal audit function at another investment management firm in Boston after it was sold by its U.S. parent company. "The organization had previously been served by a group internal audit function, so management had a mature view of what internal audit did and the value it could add," he says.

With management buy-in already a given, Sumani had to work out quickly which departments and processes needed audit focus first, as well as demonstrate that he and his newly appointed team understood the business and the risks it faced. "I needed to establish what my priorities were very quickly, and what skills and experience I would need for my team," he says.

Sumani notes that it can be a struggle for heads of internal audit to assert their authority at the beginning. Budgets can often be decided by the CFO, for example, and if they are too low, audit heads need to deliver a compelling case about why they need more resources so early on. Sumani advises an assertive approach. "Disagreements with senior management can become quite common, quite tense, and quite political," he says. "But you have to be firm—yet persuasive—and be able to demonstrate that you have the knowledge and experience to back up what you are asking for."

For example, Sumani notes that he was given a budget for seven team members and was advised to outsource the IT audit function. Instead, he wanted an experienced IT auditor, which can be an expensive hire. "In the end, I was able to get what I wanted but it was not an easy argument to win," he says. There was also pressure on him to deliver results quickly, though he wasn't convinced that the areas management wanted internal audit to address first were in fact the riskiest or the best use of audit's limited resources. "So I took a risk-based approach, which was risky for me because results were not as quick," he says. "However, the results were more appropriate and in the end the stakeholders appreciated that."

Sumani also recruited someone who had more business experience than audit experience—two years in audit but a wealth of financial services experience; plus he had worked within the business. The new hire could "speak the same language" as managers in different departments, understood how they worked, and knew the key risks their departments faced, as well as how they addressed them. "As a result, we gained management's trust very early on," he says. In fact, he hired three people from within the business based on their knowledge of organizational processes and their ability to learn internal auditing quickly.

Sumani warns against hiring certain staff members just because

60% of chief audit executives say their audit function lacks impact and influence, according to the Deloitte 2018 Global Chief Audit Executive survey.

SET THE STANDARD

Anyone setting up a new audit function should be familiar with The IIA's *International Standards for the Professional Practice of Internal Auditing.* Several standards, in particular, are especially relevant to the process:

1000 – Purpose, Authority, and Responsibility
1110 – Organizational Independence
1200 – Proficiency and Due Professional Care
2000 – Managing the Internal Audit Activity
2020 – Communication and Approval
2030 – Resource Management
2040 – Policies and Procedures
2050 – Coordination and Reliance
2060 – Reporting to Senior Management and the Board
2230 – Engagement Resource Allocation

management wants them on the team. "Choose your own team and hire who you need or want," he says. He also advises against letting management dictate what internal audit should be doing, emphasizing that it's the audit leader's job to prioritize which areas need the greatest resources and immediate focus. "If internal audit wants to show it is independent, it needs to assert that independence from the beginning," he says. "However, if you're going to ask for more resources and go up against management, be sure you can do what you say you are going to do."

THE RIGHT PEOPLE

Phil Tarling, an internal audit consultant based in the U.K. and former chairman of The IIA's Global Board of Directors, also emphasizes the importance of staffing-related decisions early on. "Any new internal audit function will live or die by the people it has on its team," he says. "The question you need to ask is whether you want more low-level people who can do the nuts and bolts work effectively and can cover a lot of basic audits across the business, or do you go for high-level people who are willing to get their hands dirty, do the low-level work as well, but who can cover less ground?" He notes the answers depend largely on management's expectations, adding that staffing decisions can have ramifications down the road as internal audit matures.

Tarling says CAEs who are asked to manage a completely outsourced function can enjoy certain advantages. He points to the increased ease of saying that audit reports received are inadequate or requesting that a particular partner or subject matter expert lead an engagement, as well as leverage in negotiating additional services.

Regardless of team composition, Tarling, like Sumani, advises a firm, proactive approach. "If you are in charge of a fully outsourced function, or if you cosource, then make sure you flex your muscle and get exactly what you want," he says.

A SOLID FOUNDATION

Setting up internal audit from scratch will always present challenges, but taking a steady and realistic approach that involves management buy-in from the start will make the process a lot easier. And to build trust and avoid confusion or conflict, it is also important to remember that internal audit must define its scope and terms of reference from the outset. Management will be more likely to respond favorably if positive early impressions are made, and more likely to trust internal audit's judgment going forward.

NEIL HODGE *is a freelance journalist based in Nottingham, U.K.*

MORE

VISIT www.theiia.org/IAFunction for IIA suggestions and resources on setting up a small internal audit function.

Internal audit's ability to serve as a trusted advisor to its primary stakeholder is key to organizational success.

Trusted advisor relationships are all the rage nowadays. Consultants in various industries have made a case for their services as trusted advisors, and the term has become part of the lexicon of internal audit. But does anyone really know what it means? No listing for it can be found in a dictionary, though informal definitions include words like *mentor*, *guru*, and *go to*. Given the term's nebulous meaning, why are internal auditors so determined to promote themselves this way? And without a universal definition, how do they know they have achieved trusted advisor status?

The answers can be found, in part, by examining internal audit's relationship with the audit committee. The committee will always be internal audit's primary stakeholder. Auditors owe it to themselves and the audit committee to maximize this relationship, and nothing

The Audit Committee *Connection*

Seth Peterson

Illustrations by Sean Yates

characterizes its ideal state better than the phrase *trusted advisor*. This status is earned over time with painstaking attention to detail—it requires effective communication, strong relationships, and a willingness to facilitate organizational change. These overarching areas form pillars of trust with the audit committee, and by examining each closely internal auditors can help determine whether they've become trusted advisors. Failures may occur along the way, but these failures can help cement the trusted advisor relationship. Getting this relationship right is essential to the organization's success.

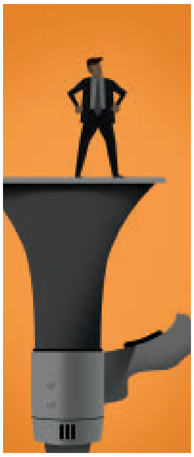
PRESENCE AND VOICE

Unlike the old adage that children should be seen and not heard, internal auditors need to be both seen *and* heard, loud and clear. They must have a presence in the boardroom, the C-suite, and wherever significant organizational decisions are made. But they shouldn't be a fly on the wall—auditors need to provide insight and promote change. They also need to know when it's appropriate to escalate an issue and push for resolution.

Have an Opinion Internal auditors can't just point to potential risks and opportunities. They serve as the eyes and ears of the audit committee, and committee members will frequently ask for their opinions. Auditors need to deliver opinions that are not only informed, but supported by facts and in line with the organization's objectives. Trusted advisors don't stop at explaining the risks and potential outcomes. When the audit committee asks internal audit's opinion on the progress or potential impact of a key initiative, auditors should be well-versed enough to provide useful, relevant information.

Engage With Passion Practitioners from the chief audit executive (CAE) down to the newest staff auditor need to be engaged and passionate about helping the organization achieve its goals. A passionate, energetic audit team

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



elicits confidence from the audit committee and shows commitment to the organization. Internal auditors can demonstrate these qualities, for example, by immersing themselves in the organization's activities and stepping outside their comfort zone. They need to bring enthusiasm and drive to everything they do — the audit committee will take notice in the internal auditors' communications and actions, as well as the results they produce.

> Auditors need to be both seen *and* heard, loud and clear, with a presence in the boardroom, the C-suite, and wherever significant decisions are made.

The Right Cadence Nobody wants a reputation for "crying wolf," but sometimes internal audit needs to be persistent to have its message heard. The audit committee needs to know internal auditors are doing their job, and at times that means delivering bad news. Early in my career, I expressed concern about a particular department's culture and the risk of it losing a large percentage of employees due to poor morale. Similar to the boy who cried wolf, my message received lots of attention at first but not nearly as much upon subsequent warning. By the third time, my prediction about staff departures unfortunately came true. If I had developed the right cadence, my message would have achieved greater impact. Internal audit can't have a trusted advisor relationship until the audit committee knows the auditors can gauge the appropriate frequency, tone, and timing for effective communications.

AGENTS OF CHANGE

While internal auditors may have a reputation for bringing awareness to important issues, how often are they the ones willing to take action and facilitate organizational change? In their capacity as advisors, practitioners can perform a great deal of change-oriented work without compromising their independence. And nothing can solidify internal audit's trusted advisor relationship with the audit committee more than demonstrating the audit function's ability to drive positive change.

Wield Personal Power The audit committee needs to know that internal audit can facilitate change based on its influence. However, influence can't be achieved solely through positional power, or the authority held by virtue of one's place in the organization's hierarchy. It must come from personal power as well, drawing on personality, knowledge, and social skills.

Positional power strategies can only go so far — often, they are effective in the short term but damage relationships and create resentment over time. CAEs who use their personal power to exert influence are much more effective. It can be a powerful tool for helping drive organizational change, establish buy-in, encourage collaboration, and foster a more positive culture. Successful CAEs rely almost exclusively on personal power, but they can also draw on positional power if needed. When

Understanding and considering risks that could affect the business ranked No. 1 in a list of 10 mandates for audit committees in Protiviti's Setting the 2019 Audit Committee Agenda report.

the audit committee sees the audit function leading change in the organization, driven by personal power, it will be more likely to view internal audit as a trusted advisor.

Speak the Language Internal auditors need to show the audit committee they are multilingual, though not in the traditional sense of fluency in foreign languages. Organizations, and even individual business units, often have their own unique language, jargon, and culture. Suppose internal audit needs to speak with the external auditors, relay a message to the IT department, and then coordinate with the head of sales. Even in the most seamless environments, what are the chances that all of these functions can easily understand each other, much less effect organizational change initiatives? Internal auditors have a wide breadth of reach within the organization that enables them to connect the dots and interpret for others. They can synthesize what one area is trying to communicate into relevant information for another. Most importantly, internal auditors can relay those communications to the audit committee. They will know they've become a trusted advisor to the committee when they can interpret highly technical or jargon-filled language and distill it into meaningful information that committee members can easily digest and act upon, creating the desired change in the organization.

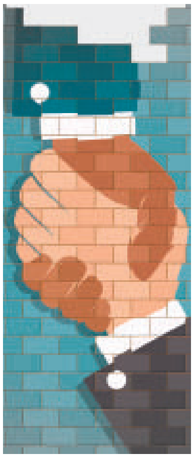
Be Proactive Taking on a project at the request of the audit committee is an easy decision. Almost all of the time, the answer needs to be yes. But trusted advisors go a step further by getting involved even before they're asked. If auditors pay close attention to organizational developments, they can proactively assess emerging priorities before the audit committee requests their assistance. Questions often arise from committee members when the organization receives negative publicity—they want assurance that the organization is protected. Trusted advisors will take the initiative to evaluate the situation, consider it carefully, and present an objective picture to the audit committee in anticipation of its queries.

RELATIONSHIP BUILDING

Relationships play a key role in establishing trust. Without adequate familiarity and comfort with the CAE, members of the audit committee may not fully leverage internal audit's capabilities. Several building blocks can strengthen audit's relationship with the committee and provide confidence in its ability to deliver value.

Nothing can solidify internal audit's trusted advisor relationship more than demonstrating the audit function's ability to drive positive change.

Maintain Integrity Auditors' integrity represents the foundation of their role as trusted advisors. The audit committee needs to have full confidence that audit practitioners are above reproach, their motives are pure, and they will act in the best interest of the organization. Without such assurance, a



trusted advisor relationship cannot exist. When faced with situations that may damage relationships, hurt the organization's bottom line, or reflect negatively on the audit function, practitioners must act in accordance with their core values. Some painful conversations may be required along the way, but the audit committee will appreciate internal audit's commitment to integrity.

Answer All the Questions When the audit committee asks questions, more pressing issues often lie beneath the surface. As trusted advisors, internal auditors must get to the root of questions — the underlying reasons behind them. For example, the committee may ask, "How receptive have departments around the organization been to implementing the new technology?" Is the question really about departments' receptiveness, or is the committee seeking to understand whether the technology has been worth the investment, or if there is a holdout department that needs to be addressed? Or perhaps it's seeking to probe an even deeper issue. Auditors will know they have achieved trusted advisor status when they answer all of the audit committee's questions, both explicit and implicit.

Back Words With Action Internal audit's status as a trusted advisor is contingent on its ability to fulfill commitments to the audit committee — every time. Auditors commit to completing audit projects as part of the audit plan, and they must back that up. They commit to performing their work with the necessary skills, abilities, and expertise, and they commit to remaining independent and objective in the process. I recall a time when our team was struggling to complete the audit plan as promised in light of late-year turnover within the function. After completion of the plan, one of the audit committee members pulled me aside and told me the deck was stacked against us — that we shouldn't have been able to complete the plan. I replied that we made a commitment and had no intention of falling short. Instant credibility was established, and the path to becoming a trusted advisor was set. Trusted advisors fulfill commitments and support their words with actions.

Several building blocks can strengthen internal audit's relationship with the audit committee and provide confidence in its ability to deliver value.

CONFIDENCE AND TRUST

Maintaining an effective relationship with the audit committee is vital to organizational success. When CAEs invest in that relationship and build a stronger connection, mutual trust and confidence is more likely to emerge. No one can become a trusted advisor overnight, but once achieved the benefits for both parties, and the organization as a whole, are well worth the effort. Ia

SETH PETERSON, CIA, CRMA, QIAL, *is vice president, internal audit manager, at The First National Bank in Sioux Falls, S.D.*

Sawyer's
INTERNAL AUDITING
Enhancing and Protecting Organizational Value
7TH EDITION

Beneath the Data

Auditing with self-service business intelligence tools can mine the organization's data sources to provide greater assurance.

Christopher Kelly
James Hao

Illustration by Edmon de Haro

Big data can tell unexpected stories: The chief financial officer who had a conflict of interest with a supplier to whom he had awarded a multimillion-dollar contract. The two employees who provided their company-supplied fuel cards to family members to refuel their personal vehicles. The executive who had an affair with a union official during wage negotiations.

Internal auditors never could have discovered such wrongdoing through traditional audit sampling, walk-throughs, or reliance on the representations of management. They were only found by using business intelligence tools to mine data sources that are now routinely available.

BUSINESS INTELLIGENCE FOR AUDITORS

Audits typically entail inquiries of management, walk-throughs, and transaction sampling as a basis for statistically inferring the effectiveness of each internal control attribute under review. To be generalizable within a given confidence interval, transaction samples need to be both large and randomized to represent the entire population. In doing so, internal auditors usually presume that the population conforms to a normal bell curve. This brings with it the risk

that if the sample is too small, the tests are performed with insufficient care, or the population is skewed differently from a normal bell curve, the auditor may form the wrong conclusions about the control's true characteristics. If the population contains any erroneous or fraudulent transactions, it is unlikely they will turn up in a walk-through or random sample.

Today's self-service business intelligence tools expand internal audit's toolkit from mere questionnaires and sampling to mining entire data populations. These tools make it easier for auditors to mine data for errors such as anomalous transactions and fraudulent data correlations (see "Mining for Errors" on page 45). In this way, auditors can pinpoint actual error, fraud, and cost savings that demand action.

Beyond financial transactions, auditors can use business intelligence tools to access newly available data sources such as telecommunications, email, internet usage, road tolls, time sheets, maintenance schedules, security incident logs, clocking on/off, and electronic point-of-sale transactions. Previously, many of these sources either were not auditable or were stored as manual records. Business intelligence tools open the door to a variety of audits.

Inventory For many organizations, inventory is a complex and poorly understood process. Organizations record movements in cash, debtors, and creditors within their financial systems. Yet, inventory data easily can get out of step with the physical daily movement of thousands of nonhomogeneous goods. Inventory is vulnerable to receipting errors, barcode misreads, obsolescence, rot, and shrinkage.

Things often go wrong in inventory, and audits often have revealed downside errors of 10 percent of inventory value. Therefore, internal audit could focus on ensuring quantity and description data matches physical reality through accurate goods receipting into the accounting system, precise sales capture, and reliable stock-taking. Once inventory data reflects the physical goods on hand, data mining can assist with identifying:

- Slow-moving and excessive inventory build-up.
- Book-to-physical adjustments pointing to shrinkage or theft by location.
- Refundable stock that can be returned to suppliers.
- Stock-outs where the organization lost sales because of insufficient demand analysis.
- Negative quantities revealing goods receipting or similar process errors.

This kind of audit analysis demonstrates the informational value of having accurate inventory data. Such information can lead the organization to prioritize which inventory processes most need fixing.

> Beyond financial transactions, auditors can use business intelligence tools to access newly available data sources.

Supply Chain Organizations need to know supplier agreements do not conceal undeclared conflicts of interest and suppliers are paid no more than their contractual entitlements. Even small organizations process thousands of supplier payments daily, so errors are likely. Data mining can include:

- Matching supplier master data such as bank account numbers, addresses, and telephone numbers to employee and next-of-kin master data for unexpected relationships.
- Isolation of purchase orders or payments just below authorization thresholds.
- Erroneous duplicate invoice payments because of optical character recognition or human error when entering invoice references such as mis-entry of "I" instead of "1," or "S" instead of "5," or "/" instead of "\."
- Historic credit notes that have never been offset against subsequent payments and remain recoverable from suppliers.

Audits using these tests have experientially revealed an average of 0.1 percent in errors, which enabled organizations to recover cash refunds from suppliers. Auditing over several prior years can result in material financial recoveries.

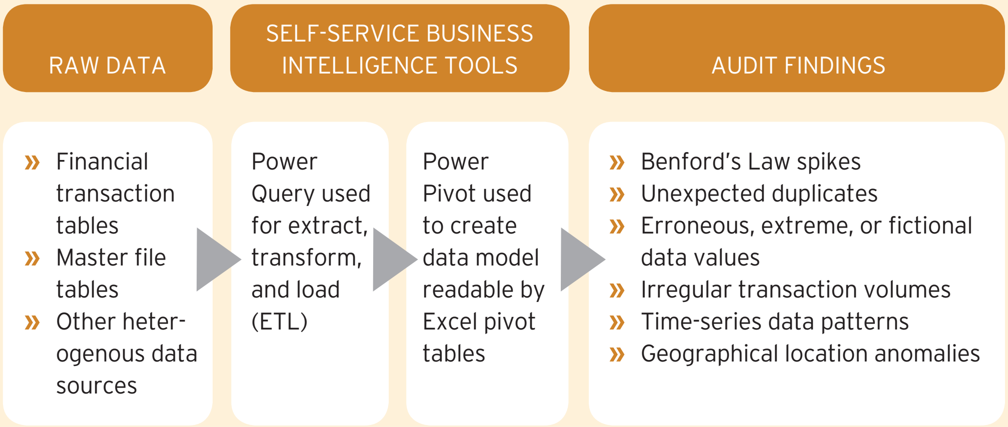
Payroll For most organizations, payroll is the largest single cost. The board and audit committee need to know overpaying or underpaying employees is minimized. Payroll data mining can include comparing hours paid to hours actually worked by matching sick leave and holiday to other time- and location-stamped data such as building entry/exit data, cell phone metadata, and email data. In doing this, internal auditors can present management with compelling evidence that supports corrective action. Moreover, previous audits have uncovered savings of about 1 percent of total payroll cost from:

- Claiming fictional hours on time sheets.
- Falsely claiming to be working at home or on paid sick leave.

Data quality and management, discovery and visualization, and self-service business intelligence are the most important business intelligence trends, the BARC BI Trend Monitor 2019 reports.

MINING FOR ERRORS

The diagram below summarizes the steps from raw data to audit findings when internal auditors use Excel's Power Query and Power Pivot features.



RAW DATA

- Financial transaction tables
- Master file tables
- Other heterogenous data sources

SELF-SERVICE BUSINESS INTELLIGENCE TOOLS

Power Query used for extract, transform, and load (ETL)

Power Pivot used to create data model readable by Excel pivot tables

AUDIT FINDINGS

- Benford's Law spikes
- Unexpected duplicates
- Erroneous, extreme, or fictional data values
- Irregular transaction volumes
- Time-series data patterns
- Geographical location anomalies

- Missing scheduled training.
- Finding repetitive patterns of fictitious sick leave taken on Mondays, Fridays, and the day before or after public holidays.

Company Motor Vehicles Auditors can mine data gathered from vehicles, including road tolls, refueling, traffic penalties, and insurance claims. This jigsaw puzzle of data can show auditors how vehicles are being used for business purposes, possible abuse of vehicles, and drivers with poor driving histories that result in unnecessary cost. This data can be obtained from external motor fleet providers and insurers. Such audits can recover around 5 percent of fleet costs.

Metadata While the content of company-issued cell phone calls and text messages is confidential, the accompanying nonconfidential metadata includes called numbers, durations, date and time stamps, and base station geographical locations. Auditors can discern employee activity, interconnections, and external relationships during work hours or while on paid sick leave by matching this metadata to other sources such as the organization's telephone list and employee and supplier master files. Internet usage metadata provides similar insights. These data sources can help when investigating white collar conflicts of interest and fraud.

These are just a few areas where business intelligence opens new portholes. Partnering with the chief information officer can help internal audit access the organization's databases. Once access is granted, auditors can use business intelligence tools with minimal assistance.

GETTING STARTED

With business intelligence, auditors are no longer constrained by Microsoft Excel's 1,048,576 row limit. Excel 2016 includes built-in business intelligence tools, Power Query and Power Pivot. Power Query is an extract, transform, and load (ETL) tool that reads source data and makes it available for Power Pivot for data modeling. This source data typically comes from comma- or tab-separated outputs from other systems. Auditors can access Power Query under Excel 2016's Data ribbon, where it is also known as Get Data and, once opened, Query Editor.

Power Query and Power Pivot have formula languages that allow users to create new data columns specific to their own unique needs. Power Query uses M formula language and Power Pivot uses Data Access Expressions (DAX). Both languages differ from Excel formulas. Whereas Excel formulas are not case sensitive and usually do not distinguish among string, date, and numeric data types, M and DAX are sensitive to both text case and data type. This distinction is important when manipulating data and performing calculations.

Once internal auditors have loaded and edited the raw data down to only the needed columns in Power Query, they can add each table to the Power Pivot data model under the "Add to data model" option. Auditors can then access Power Pivot from Excel under "Manage data model." From there, they can use the "Diagram view" to link tables such as transaction files keyed to their corresponding master files. The data model can handle multiple external data

APPLYING BUSINESS INTELLIGENCE USING BENFORD'S LAW

The steps below illustrate how business intelligence tools can enable internal auditors to use Benford's Law to annotate original source data with leading digits. Leveraging Power Query, Power Pivot, M, DAX, and standard pivot tables together can produce audit insights.

STEP 1. Using a data-cleansed table created in Power Query, create additional field columns using "Add column/custom column" to capture the leftmost 1, 2, 3, etc. digits for Benford's Law analysis.

Data mining learning point: *Being able to create custom columns in the data model is key to internal audit's ability to generate original insights. Auditors should not create too many new columns or the data model may become unmanageable within their computer's memory limits.*

STEP 2. To avoid picking up the dollar-cent decimal points, multiply the amount field by 100 to convert it into whole cents and then use an M formula to convert the absolute amount to text and pick up the two (or three or more) leftmost digits. For example:

```
= Text.Start(Text.From(Number.
    Abs([Amount]) * 100), 2)
```

Data mining learning point: *In this M formula, auditors are isolating the two leftmost digits and "[Amount]" is the literal field heading from the source text file. Note that the formula syntax differs from Excel.*

STEP 3. Once the desired Benford analysis columns have been created in Power Query, refresh the data model in Power Pivot.

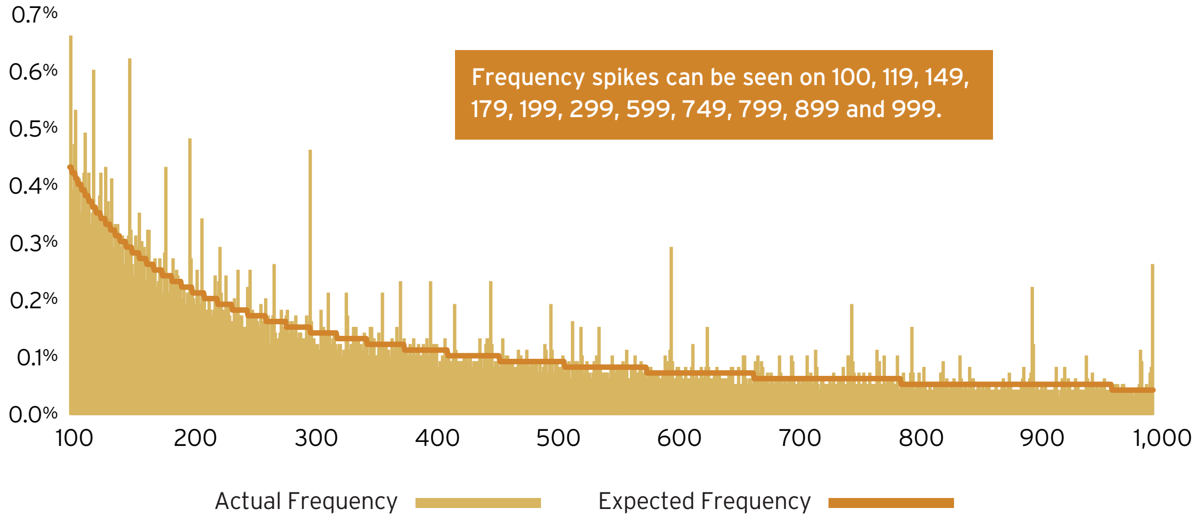
Data mining learning point: *Now that the raw data is in the Power Pivot data model, auditors can access the entire table, including the new column added in Step 1 within Excel's standard pivot tables.*

STEP 4. Show the leftmost digits using the pivot table's "Show Values As/% of Grand Total" and compare this to the expected logarithmic frequency under Benford's Law. Then, visualize the resulting columns with a chart to highlight spikes between actual and expected frequency.

Deviations are most likely to have occurred where a systematic weakness has been exploited repeatedly.

Data mining learning point: *Double clicking each deviant spike in the pivot table will display all the individual transactions that caused the spike, which auditors can then scrutinize for irregularities. In this way, Excel can instantly find the deviant transactions from a huge data population.*

BENFORD'S LAW FIRST 3 DIGITS ACTUAL TO EXPECTED FREQUENCY – INVOICES



Frequency spikes can be seen on 100, 119, 149, 179, 199, 299, 599, 749, 799, 899 and 999.

87% of organizations have low business intelligence and analytics maturity, yet Gartner estimates self-service analytics and business intelligence will produce more analysis than data scientists in 2019.

sources as well as normal Excel tables. This capability allows auditors to create multidimensional relational databases rather than two-dimensional flat files.

Power Pivot enables auditors to annotate the relational databases retrieved in Power Query with unique columns and measures specific to audit needs, which can be analyzed using Excel's pivot tables. "Applying Business Intelligence Using Benford's Law" on page 46 illustrates how Power Query, M, Power Pivot, and Excel can work together to search for irregularities.

DATA CLEANSING

Data files usually need to be cleansed before analysis. That is because over time, original source data is input by a variety of users whose training and attention to accuracy may be inconsistent. Some fields may hold invalid data as a result of being migrated from different systems or different versions of the same system. Moreover, stack overflow and other error types may lurk in historic data, the text files may have misaligned some fields, and records may be broken across two or more rows.

> **Internal auditors should keep a record of data cleansing actions in case future rework is required.**

Comma-separated text files can present extra cleansing problems if users have input commas into individual fields. For example, "Kelly & Yang, Inc" would translate into two separate fields because of the comma, whereas "Kelly & Yang Inc" would translate into one field.

ETL tools will attempt to read all transactions from the raw data files. But if the tool encounters errors, it may exclude them from the upload, resulting in loss of data that dilutes the objective of testing the entire population. If time allows, the auditor may cleanse the text files field-by-field in a spreadsheet or word processor by rejoining broken records, recalibrating misaligned fields, trimming stray characters or spaces, replacing known error values with blanks or zeros, and converting dates stored as text to real dates.

Further cleansing may be required if source files are fragmented across different years or subsidiaries and need to be joined into a single table, or if source files are tabulated differently from how internal audit wants to use them. In the first case, Power Query can append files into a single data source provided the field headings are identical. In the second case, auditors can untabulate inappropriately tabulated source files back into a single column of data using Power Query's Unpivot command.

Internal auditors should keep a record of data cleansing actions in case future rework is required. Any updates to source data made in Power Query will need to be refreshed in the Power Pivot data model as well as in dependent pivot tables.

EFFICIENT QUERIES

Business intelligence tools are faster than previous versions of Excel, but internal auditors still need to be mindful of formula efficiency. If the auditor tries to add a new calculated field to a data model that requires a row-by-row lookup of each element in a two-million-row database, that could easily result in two million x two million = four trillion separate lookups.

Even with software, four trillion lookups could take several hours. Auditors can increase query efficiency by indexing, compartmentalizing a large query with efficient calculated fields, and filtering out unwanted columns or transactions that are blank or below a given materiality threshold.

SECURING DATA

To avoid internal audit being the source of a leak, or to limit the damage if the unthinkable occurs, auditors should take care with data. Auditors can exclude fields that identify living individuals, home addresses, or bank account numbers from downloads or replace them with codes such as an employee number instead of a name. They should be cautious when transmitting data to ensure USB drives are secure and electronic data is not emailed to unintended recipients. Auditors should check recipient email addresses before hitting "send." Password protection and encryption should be used when practical. As auditors only need to work on copy data—rather than live data—they usually can destroy their version and wipe USB drives after the audit is completed.

ORIGINAL INSIGHTS

Business intelligence tools unlock new ways to audit. With only a little new learning, business intelligence tools can expand internal audit's adventures into new pools of financial and operational data that may reveal risk and control insights. Moreover, because even the most innocuous transactions leave data trails, imaginative analysis can uncover errors, fraud, and cost savings that transform audit reports into compelling reading for executives and the board.

CHRISTOPHER KELLY, DPROF, FCA, MIIA, *is partner at Kelly & Yang in Melbourne, Australia.*

JAMES HAO, CPA, *is an associate at Kelly & Yang in Melbourne.*

An Audit of

Matej Drašček
Adriana Rejc Buhovac
Gavin Lawrie

The *International Standards for the Professional Practice of Internal Auditing* and The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management–Integrating With Strategy and Performance* emphasize strategy as the basis for internal audits. Despite this, auditors still often lack the tools and methodologies to audit strategy development and implementation for their organizations. By understanding the needed competencies for tackling a strategy audit, internal audit can help improve governance, risk management, and internal controls in an organization's strategic management process.

Strategic management process best practices typically consist of four interdependent steps:

1. Identify owners' (key stakeholders) expectations.
2. Analyze the broader environment, industry, and organization's performance.
3. Develop a long-term vision (destination) and strategy leading to that vision, as strategies reveal causality between strategic activities and strategic outcomes.
4. Implement strategy via communication, performance measurement and control, and review meetings.

While it is not the role of internal audit to validate the content of these steps as performed by the organization's leadership, there is an important requirement for the internal audit function to confirm that each step is being undertaken, and that the organization is using sensible methods at each stage. It is also important for the internal audit team to confirm that these steps are happening concurrently, with each of them operating consistently and cooperatively.

QUESTION 1: HAVE STAKEHOLDERS' EXPECTATIONS BEEN IDENTIFIED?

Even though the idea of shareholder maximization is always present, business practice abounds with examples of owners balancing profits (financial goals) with other goals—including corporate social, environmental, and economic performance. The first step of auditing strategy is to assess whether the board and senior management have identified stakeholder expectations of future performance in some practical way and have incorporated a response to these expectations within their strategy development process. In the long term,

Strategy

Four questions can help internal auditors ensure an effective strategic management process, the backbone of organizational success.

the achievement of stakeholder expectations is the ultimate measure of the performance of the organization's senior management team. It should serve as stakeholders' basis for evaluating whether the organization is being managed effectively. As such, it is vital that the strategy focuses on either meeting stakeholder expectations directly, or building and managing a supportive consensus within the stakeholder community concerning the choices of which expectations to meet over time.

QUESTION 2: DOES STRATEGY LIE ON FIRM, ANALYTICAL GROUND?

Internal auditors should focus on the most important methodological aspects of strategic analyses.

Is data reliable, relevant, and sufficient? With information easily accessible via the internet, internal auditors should assess if the information gathered is reliable and from trustworthy sources. They also need to evaluate whether the data is relevant (likely and impactful) and sufficient.

Have managers avoided the risks of overconfidence and confirmation bias? Managers are often overconfident about the accuracy of their forecasts and risk assessments and far too narrow in their assessments of the range of possible outcomes. They frequently compound this problem with confirmation bias, which drives them to favor information that supports their positions (typically successes) and suppress information that contradicts them (typically failures). They might anchor their estimates to readily available evidence despite the known danger of making linear extrapolations from recent history to a highly uncertain and variable future. Internal auditors should use professional skepticism to assess the quality of collected data.

Have potential black swan and black elephant scenarios been considered? Black swan events, such as terrorism or natural disasters, are difficult to predict and have major impact on the organization. Black elephant events, such as financial crisis cycles and climate change, are predictable, detrimental events that people or society choose to ignore. Internal auditors should assess whether the analytical process has addressed these unlikely events.

Have analysts identified historical information and emerging trends? Big data has become a necessity rather than an advantage. Organizations should analyze readily available data from public sources and also use predictive analytics, prescriptive analytics, or autonomous statistics. These approaches go beyond what and why

FLAMINGO IMAGES / SHUTTERSTOCK.COM

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

something is happening to address what will happen next.

Have the organization's current capabilities been analyzed formally? An organization's ability to satisfy stakeholder expectations is to some extent determined by the capabilities (technological or marketing, for example) of the organization. If the capabilities are sufficient, the challenge is how to deploy them to best satisfy expectations. If the organization does not have the right mix or sufficient capabilities, the strategy will need to include steps to expand and develop internal capabilities or to purchase the required capabilities from elsewhere. How will this support or hinder work to satisfy stakeholder expectations?

Is a strengths, weaknesses, opportunities, and threats (SWOT) examination an appropriate summary of key analytical findings? Internal auditors should assess whether the identified strengths and weaknesses are supported by an objective measurement or assessment, and whether the identified opportunities and threats are related to external factors—such as events from the broader environment or industry.

QUESTION 3: HAS STRATEGY DEVELOPMENT FOLLOWED BEST PRACTICES?

First, strategy development involves clearly articulating the organization's final destination (vision) at some future date. Internal auditors should assess whether the organization's vision statement addresses owner/key stakeholder expectations, is achievable and measurable, and focuses on what the organization needs to achieve vs. what it needs to do.

Second, internal auditors should check whether the strategy reflects a business case, the logical causality between strategic activities and strategic outcomes (goals). Best practice strategies include cause-effect connections (strategic linkage models) outlining causality between strategic activities, themselves, and between strategic activities and strategic goals. They also should check whether strategic goals include financial and nonfinancial goals related to the activities the organization will need to implement the changes required by the chosen strategy. This includes short-term outcomes that the organization can track to confirm the actions taken are working as expected. In addition, auditors should assess whether clear, long-term strategic goals are quantified and associated with a specific time frame. Long-term goals help the organization pick and set targets for the amount of activity that needs to be delivered and the time frame for realizing required outcomes.

Third, internal auditors should assess the documentation of strategic activities. This should include at least:

- The owner or person responsible for effective completion of a strategic activity.
- Tasks to be completed.
- Timeline of activity.
- Financial and other resources.
- How to mitigate the main risks.

Finally, internal auditors should check whether managers have ensured strategic alignment or the cascading of a designated strategy throughout the organization. Cascading is the process by which the ultimate goals are broken down into individual departmental activities, allowing for a more engaged and accountable workforce. Internal auditors should assess the responsibilities and ownership of execution plans at lower levels for implementation decisions.

QUESTION 4: IS STRATEGY BEING IMPLEMENTED?

The last part of a strategy audit is implementation. Empirical research shows that strategy implementation remains elusive regarding effectiveness, with a reported fail rate of 50 percent to 90 percent. Internal auditors should be alert to the main causes of strategy implementation failure.

Communication Effective communication plays a critical role in aligning the whole organization with the strategy and giving employees an understanding of the pace of change that will be required. Internal auditors should: 1) identify communication channels that senior management is using to support strategy execution; 2) assess the appropriateness of communication channels from the perspective of frequency and reach; and 3) check whether any guidelines or a strategy execution model exists. Internal auditors can use a modified approach to COSO's updated ERM framework to evaluate the strategy communication process.

Performance measurement and control Strategic performance measurement systems support adequate information sharing among individuals or the business units responsible for strategy execution. Internal auditors should identify whether strategic activities and goals have at least one performance indicator and target values (milestones) to keep track of what has been achieved. Then, auditors should assess the appropriateness of key performance indicators to make sure they are measurable, relevant, and informative.

Review meetings Organizations often lack senior management support in strategy execution. To encourage participation and support, senior management should set up and manage the review meetings. Internal auditors should check the frequency of the meetings, assess whether any controls have been put in place to ensure implementation actions are carried out, and evaluate whether any actions

35% of senior executives rank developing strategy implementation skills among executives as a very high priority in the Project Management Institute's Pulse of the Profession 2018.

KEY STRATEGY DEVELOPMENT AND IMPLEMENTATION RISKS

QUESTION	MAIN AUDIT RISKS TO GUIDE INTERNAL AUDITORS
Have owners' expectations been identified?	» Owners' expectations are not clear. » Board and top managers are not familiar with owners' expectations.
Does strategy lie on firm analytical grounds?	» The SWOT analysis has been produced subjectively, without objective analytical methods and data gathering. » The strategic analyses used unreliable sources, so the data is irrelevant and insufficient. » Key analytical findings have been identified based on overconfidence and confirmation bias. » Analytical findings are built on extrapolations from past events without considering unlikely, but highly impactful, events.
Has strategy development followed best practices?	» The organization has unclearly articulated its final destination (unspecified goals and no time reference). » The organization has a vague strategy. The goals are unclear and there is no causality between strategic activities and strategic goals. » Management has not established clear priorities regarding key strategic activities. » Strategic activities are not documented appropriately and are lacking activity owners, task descriptions, timelines, or identified risks. » Cascading of strategy does not exist – responsibilities for execution plans are not clear.
Is strategy being implemented?	» Information-sharing between individuals or business units responsible for strategy execution is poor or inadequate. » Communication of responsibility for execution decisions or actions is unclear. » There are no feelings of ownership of a strategy or execution plans among key employees. » There are no guidelines or models to guide strategy execution. » Upper management support of strategy execution is lacking. » A comprehensive strategic performance measurement system – a system of measurable key performance indicators with target values (milestones) for tracking progress along strategic activities and strategic goals – is missing. » There are no review meetings to assess the need for active interventions and action modifications to ensure strategy implementation.

have been modified to ensure strategic goals are reached.

PROVIDING REASSURANCE

Stakeholders—who can directly or indirectly influence the organization's ability to operate—comprise a mix of interested parties, including financial owners, regulatory bodies, and communities impacted by the organization's activities. A critical responsibility of senior management is to balance the potentially conflicting interests of these stakeholder groups and direct the organization to maximize the extent to which these interests are satisfied. Organizational strategies document the plan to modify and adapt the performance of the organization in light of these stakeholder expectations. The role of internal audit is not to validate or contest the content of the strategy—which is the responsibility of senior management—but to reassure the senior team that its approach to strategy development and implementation is appropriate and well-controlled.

MATEJ DRAŠČEK, CIA, CRMA, *is the chief audit executive at LON Bank d.d. in Kranj, Slovenia.*

ADRIANA REJC BUHOVAC, PHD, *is a professor in the Faculty of Economics at University of Ljubljana in Slovenia.*

GAVIN LAWRIE *is managing director at 2GC Active Management in Maidenhead, England.*

7 Practices for Better Audit Outcomes

The U.S. Department of Homeland Security follows guidelines aimed at improving the auditor-auditee relationship.

Jim H. Crumpacker

When it comes to ensuring successful audit outcomes, the two parties involved—the auditors and the auditees—must be committed to active cooperation. Throughout my career, I have followed certain principles that, when consistently adhered to by both parties, have resulted in successful audits.

I have worked in the U.S. Air Force Audit Agency and in the Office of Inspectors General (OIGs) of both the U.S. Postal Service and Department of Transportation. Since 2010, I have served as the director of the U.S. Government Accountability Office (GAO) OIG Liaison Office for the U.S. Department of Homeland Security (DHS). In my current position, I facilitate nearly 250 GAO and various OIG performance audits at one any time across DHS.

These seven principles, along with approaches DHS uses to implement them, can easily be used by other organizations seeking to improve their audit outcomes.

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

Believe Audits Make Things Better

This foundational principle requires auditors and auditees to believe in the work they are doing and remember that it's not just a job. Auditors and auditees must do the best they can with a view that the results of their efforts will add value to something greater than themselves. For many at DHS, believing this translates into knowing that audit's efforts are helping make the department's programs, operations, and activities more effective, thereby ensuring the U.S. and its citizens are safe and resilient against terrorism and other hazards.

Tone at the top in both the audit and audited organization is crucial to successfully implement this principle. For example, senior leaders in the audited organization must have processes in place to demonstrate a personal awareness of, and an active interest in, the audits occurring within their organization. To facilitate this, DHS assigns a priority of 1, 2, or 3 to each audit using broadly defined criteria supplemented by professional judgment and experience. Criteria include considering the level of taxpayer funding in a particular program or initiative and the significance of potential violations of statutory or regulatory requirements. Priority 1 audits warrant secretary or deputy secretary of DHS attention; Priority 2 audits are those that can be monitored at the component or headquarters directorate level, such as by the administrator of the Federal Emergency Management Agency; and Priority 3 audits are considered less critical and can be monitored at the program office level. The priority assigned to an audit is subject to change, depending on circumstances, as the audit progresses through its life cycle.

Understand and Respect Audit Independence

Arguably, one of the least understood audit standards is the U.S. Generally Accepted Government Auditing Standard of Independence, which establishes a foundation for the credibility of the auditor's work. Independence allows audit opinions, findings, conclusions, judgments, and recommendations to be impartial and viewed as such by reasonable and informed third parties. Independence requirements relating to the audit organization and individual auditor—including what independence of mind or in appearance means—and how professional skepticism is correctly defined, can be difficult to fully understand. When auditees have trouble with these or other aspects of independence, they usually just need to learn more about the concept. It is more problematic when auditors do not fully understand what independence is and is not.

During my more than 30-year career, I have seen instances of auditors knowingly or unknowingly misapplying the independence standard as leverage in an attempt to get whatever they wanted, thereby impeding successful audit outcomes. For example, some auditors have told auditees that if they did not immediately produce exactly what they asked for, or let the auditors come and go throughout the organization whenever they wanted, then the auditee was impinging on audit independence. This is quite an overreach. One way DHS mitigates misunderstandings about independence is through an annual joint DHS-wide town hall meeting hosted by the DHS under secretary for management with the inspector general and attended by audit staff, agency leadership, and program officials. The meeting's question-and-answer format provides an opportunity to openly discuss topics such as independence and, more importantly, to correct misunderstandings. Without audit independence, the value of an audit is considerably diminished; auditors and auditees need to be in sync on independence and why it is needed.

Be Open and Transparent

There should be no secrets when working with auditors. Honesty is the best policy, even if being less than open and transparent may seem more expedient in the short term. Making sure there are no surprises at the end of an audit goes a long way toward ensuring successful audit outcomes. The audit life cycle can be long, sometimes taking a year or more from research, announcement and entrance, fieldwork, summarization, report writing, A key change in the 2018 Yellow Book includes updated independence requirements for auditors who prepare the financial statements of an audited entity.

exit, and management response, to final report publication. Ample opportunities exist throughout the life cycle for auditors and auditees to allow the truth to wander. This may involve something the auditor wants to know, such as how a specific aspect of an internal control system might actually be functioning, or something the auditee wants to know, such as what findings and recommendations the auditor might be thinking about including in the final report.

DHS designates an executive-level senior component accountable official (SCAO) for audit activities within each component and headquarters directorate. SCAOs have wide organizational influence—typically at the chief of staff level—and also are responsible for, and have authority over, their respective organization's audit activities. The SCAO enables and assists program officials, audit liaisons, and others with all aspects of the audit process, including helping to resolve issues that could endanger open and transparent relationships with auditors. For example, SCAOs have mediated disputes concerning what sensitive records may be shared with GAO and OIG auditors.

4

Be Responsive

Successful audit outcomes require a commitment to work collaboratively with the other dedicated professionals involved with the audit. Responsiveness means reacting quickly and positively, and generally reflects how much someone cares about something. For example, consider how auditors and auditees respond to information requests from one another.

One way to help ensure success is to set clear expectations for these interactions and adhere to them. Senior departmental leaders at DHS have consistently articulated expectations for the entire workforce regarding cooperation with GAO and OIG, including their contractors. To maximize effective implementation of this guidance, auditor-to-auditee communication is streamlined and, as a matter of practice, audit issues are addressed at the lowest organizational level possible, trusting and empowering staff and elevating matters to more senior leadership only when necessary. This involves a certain degree of risk—for example, sometimes auditors do not receive the most fully informed response to their questions—however, DHS has found the risk to be acceptable given other controls implemented to balance the risk for the benefit of both parties.

5

Stay Engaged

Early and continuous involvement can be difficult, especially for auditees, because audits can require significant time and are not part of their primary day-to-day responsibilities. However, if auditees believe audits make things better, they will give them an appropriate level of attention among competing mission-related priorities and demands. Likewise, auditors should be mindful that continuous and effective communication with auditees ultimately enhances the flow of information and exchange of ideas. Auditors also need to be understanding about responsiveness lag when other auditee duties occasionally take precedence over the audit.

One way DHS engages with GAO and OIG during the audit life cycle to help ensure successful outcomes is through a standardized technical comments process for communicating and documenting management feedback on auditor statements of fact, notices of findings and recommendations, and discussion or draft reports. Auditors receive and consider these comments, seek clarification when needed, and make changes to work products, as they deem appropriate. The comments are not intended to substantively alter audit findings, conclusions, or recommendations. Instead, they are meant to strengthen work products by improving accuracy and context, preventing the inadvertent disclosure of sensitive information, helping validate actionable recommendations, and minimizing the number of disagreements. As a result of this process, DHS officials rarely find themselves questioning audit report narratives once published and distributed to the U.S. Congress and the public, including the media. Rather, conversations focus on what is being done to implement recommendations.

Prepare Detailed Management Responses to Audit Reports

Management responses can contribute to successful outcomes if they clearly document management's position on the findings and recommendations, identify the corrective actions that will be taken (with estimated completion dates), and assign responsibility for those actions. Auditors generally include management responses verbatim in an appendix to final reports, which are then widely distributed inside and outside the organization. Well-written management responses represent an opportunity to demonstrate how seriously the auditee takes audits. Also, when considered with the auditor's evaluation and analysis of the response—which provides additional audit perspectives on management's comments and is included in the final report—management responses provide a good roadmap for recommendation closure and the resolution of disagreements.

DHS requires a written management response for all audit reports with recommendations. Responses must:

- Clearly state agreement or disagreement (concur or non-concur) with individual recommendations. Partial concurrences are not allowed and it is acceptable to non-concur as long as the rationale for doing so is included.
- Specifically identify the organization and office responsible for taking the corrective action, such as the U.S. Customs and Border Protection Office of Field Operations.
- Outline what will be done to implement the recommendations—including proposing alternative corrective actions if program officials believe these would be more effective. This is typically stated in terms of actions completed, ongoing, or planned, being sure to address all aspects of each recommendation.
- Include an estimated completion date for each action, which can be up to 12 months beyond the estimated date of the final report, or longer if interim milestones are included at approximately six-month intervals.

Actively Follow up on Recommendation Implementation

DHS and its auditors view audit follow-up as a shared responsibility and an integral part of good management. This view has significantly improved and facilitated positive interactions among auditors and auditees. DHS devotes substantial attention to taking corrective actions on audit findings and recommendations, a practice that is essential to improving operational effectiveness. This requires sustained leadership commitment at the highest levels. For example, the DHS deputy secretary and/or the under secretary for management meet with the SCAOs every two months to review and discuss the status of ongoing audits, open recommendations, and related performance measures. Senior leadership also receives various periodic audit status reports in between these meetings, including a biweekly Priority 1 report.

If DHS management commits to an action in an audit response, it does its best to follow through on that commitment timely. DHS also strictly adheres to a practice of not closing any GAO and OIG audit recommendations without first reaching agreement with the auditors. This provides Congress and the public added confidence that appropriate actions have been taken to implement these recommendations or otherwise resolve any disagreements. As a result, DHS averages less than one recommendation annually that requires formal resolution.

A POSITIVE APPROACH

Successful audit outcomes do not just happen. The participants must believe audits make things better and be mindful of the six other principles for ensuring successful outcomes. Moreover, auditors and auditees have a fundamental responsibility to ensure that the resources expended on audits provide a positive return on investment for stakeholders. Ia

JIM H. CRUMPACKER, CIA, CFE, *is director of the U.S. Department of Homeland Security's GAO-OIG Liaison Office in Washington, D.C. This article represents the personal views of the author and not necessarily those of any U.S. government department or agency.*

Board Perspectives

BY MATT KELLY

IT'S ALL ABOUT TRUST

Audit committees and CAEs work best when they pledge to work together.

THERESA GRAFENSTINE

MARTY COYNE

BRENDA GAINES

Audit committees and chief audit executives (CAEs) talk constantly about how to foster more engagement with each other, and rightly so. Their relationship is one of the most important for an organization to get right, if it wants effective corporate governance.

A good place to begin, then, is to consider the origin of the word *engagement*. It descends from the French verb *engager.* Today that word means "to hire" or "to employ"—but 400 years ago, when *engagement* first crept into the English language, *engager* actually meant "to pledge."

That's a useful point to remember when contemplating how to improve the relationship between audit committee and audit executive. It's about pledging to be there for each other: I will help you, and you will help me, *and we both know that.* In other words, it's about trust. Audit committees and audit executives have to trust that the other is thoughtful, competent, and looking out for the best interests of the organization.

That's all the more true today in an immensely complex modern business world. Audit committees have a fiduciary (and for publicly traded companies, statutory) responsibility to oversee risk management at their organizations. Audit executives are watching their profession transform from an older era of financial statement audits to a newer one of monitoring risk and working with other parts of the organization to manage risk (see "The Audit Committee Connection" on page 36.)

In other words, both parties now have more to do, and more to worry about. That's why cultivating a strong working relationship is important. That's why *fostering trust* is important. Each needs the other to succeed.

"It's a whole new world," says Theresa Grafenstine, a managing partner at Deloitte, audit committee chair of the Pentagon Federal Credit Union, former audit committee chair of ISACA, and former inspector general of the U.S. House of Representatives. "We need to see this as a partnership."

Trust Begins With Communication

For starters, audit committees and audit executives can simply talk more often. There should be executive sessions at the end of audit committee meetings without management present. The audit committee chair should schedule informal chats with the CAE between formal meetings, even without anything specific in mind. Talk.

Marty Coyne, audit committee chair at Ocugen and a past audit committee member at numerous other technology companies, swears by both practices. "It's almost mandatory in my mind," he says. "If the audit

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

committee isn't doing that, shame on them." (In the most recent North American Pulse of Internal Audit survey, nearly one-third of audit executives say they do *not* meet in private session with the audit committee.)

What questions should audit committees put to CAEs in those sessions? Unless some specific issue demands attention, they should pose open-ended questions without any right or wrong answers. What's been happening in the last quarter? Are there any challenges where they can help? Coyne's go-to question in such meetings: "What *didn't* you say?"

Those questions give the CAE a chance to speak his or her mind, and to lead the discussion where the CAE believes it should go. "It's so you can draw that person out," says Brenda Gaines, audit committee chair for Tenet Healthcare. That, in turn, can foster the CAE's trust in the audit committee.

The audit committee's job is to ensure differences of opinion are aired openly.

Audit committee chairs should take the extra step of regular communication with the audit executive beyond the standard audit committee meetings. Gaines schedules a monthly phone call; Coyne has met CAEs for coffee. However the chair does it, that casual, unstructured line of communication can be invaluable.

"It would help me frame out the agenda for the audit committee meeting," Coyne says. After all, audit committees have plenty of risks they can discuss in a formal meeting, and time is limited. So Coyne would chat with the audit executive to pinpoint which risks (aside from any standard matters about financials, investigations, and so forth) truly warranted the audit committee's attention.

"There's always room for a topic," Coyne says, "and I want to make sure that the topic we talk about, beyond the normal topics, is germane and important, and going to move the needle."

Trust Endures Difficulty

All that communication and trust spadework can pay off in several ways. First, the very act of creating an open culture among senior executives and the audit committee reduces the chance that difficult matters will arise where the audit committee needs to "take sides" in an impasse between internal audit and management. Second, when those impasses *do* arise (spoiler alert: sooner or later, they will), the audit committee can resolve it with the least amount of acrimony.

That also means the audit committee needs a healthy relationship with management, and needs to ensure management and the CAE have a healthy, respectful relationship, too. Grafenstine calls it the "triangle of success"—each side having equal power, where they each understand the other's roles and responsibilities.

Coyne's approach is, whenever possible, to bring all sides together in open communication at a committee meeting. After all, the CAE may be disappointed with the pace of improvement in a business process, but management might have a good reason for the delay: product launches, sudden departure of key personnel, or some other operational issue.

The audit committee's job is to ensure such differences of opinion are aired openly and respectfully. The best way to do that is to foster trust long before that conversation happens.

"What you don't want is all sorts of back-door conversations going on," Coyne says, like the CEO and CAE speaking to the audit committee members separately, but not to each other. "That's a disaster when that happens."

An Environment of Trust

That need for collegial relations with management raises another point. From today into the future, success as a CAE will be more about exercising leadership and working with other parts of the organization to manage risk, rather than technical mastery of audit techniques.

Good audit executives "are not only a valuable resource to help the audit committee discharge its duties," Gaines says. "They provide management with valuable insight as well on whether risk mitigation is effective."

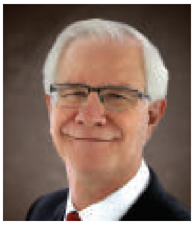
Those risk issues can range from IT controls for cybersecurity, to successful integration of an acquisition, to the rapidly rising concern of "culture risk." Business processes might need improvement. Data analytics might provide valuable insights that someone needs to translate into updated controls and practices.

A good audit executive *can* do all of that, even while balancing the need for independent analysis of risk issues—*if* the audit committee fosters an environment of trust and open dialogue, and assures that the CAE has the resources he or she needs (financial, technological, personnel) to do the job.

It's a lot to ask, of the audit committee and CAE, alike. One might almost say the French had it right 400 years ago: Engagement really is about pledging yourselves to each other. Ia

MATT KELLY *is editor and CEO of Radical Compliance in Boston.*

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



BY J. MICHAEL JACKA

WE ARE NOT AUDITORS

Practitioners should not let themselves be defined by just one word.

How do you respond when asked, "What do you do for a living?" It shouldn't be tough, but answering that question can be an exhausting exercise in diplomacy and obfuscation. If you say that you are an auditor, almost inevitably the person then asks, "Oh, do you work for the Internal Revenue Service?" Or some may just suddenly disappear in search of what they believe will be a more interesting conversation — such as the rate of moss growth on redwoods or observations on the drying of paint. Even if they don't run away, their eyes have usually rolled to the back of their head by that point as they check out of the conversation, mentally filing your mug shot in The Hall of Individuals With Whom I Will Never Talk Again. All because of one word — auditor.

English comedian and actor Stephen Fry once said, "We are not nouns, we are verbs. I am not a thing — an actor, a writer — I am a person who does things — I write, I act — and I never know what I am going to do next. I think you can be imprisoned if you think of yourself as a noun."

And therein lies the problem. We describe ourselves as a noun. We make ourselves a thing. And by thus naming ourselves, we become that thing. We are auditors. We conduct audits. We perform audit work. We produce audit reports. We are part of an audit department. Our identity and our future become inextricably intertwined with the concrete solidity of a thing that has been named.

Instead, we need to define ourselves as verbs. We need to identify with what we do, not what we are. And that means we need to describe ourselves to others by talking about what we do, not what we are. The next time someone asks what you do for a living, try one of these:

"I work with executive managers to help ensure they achieve their objectives."

"I help streamline processes to ensure management succeeds."

"I provide oversight to help the organization succeed."

"I work with management to help eliminate problems before they occur."

Any one of these will lead to a better conversation, speak to the value internal auditing can provide to an organization, and keep the other person from scuttling away like a lobster confronted with a pot of boiling water.

I am not suggesting that we no longer use the title *auditor*. But we have to identify ourselves in a way that helps us and others understand we are free to be more. We provide assurance; we consult; we advise; we fulfill the mission, principles, and definition of internal auditing that help establish who we are. When we realize we are not just auditors — when we make the transition away from being a noun — we are free to be the verbs that describe the real value we provide. 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

THE FORWARD-LOOKING AUDITOR

Foresight is a skill internal auditors need to master in today's disruptive business environment.

SHAWN STEWART
Partner and National Controls Advisory Practice Leader
Grant Thornton

SANDY PUNDMANN
U.S. Internal Audit Leader
Deloitte

Why is it so important for internal auditors to add foresight to their job description?

STEWART Disruptive technologies and the trends impacting business are expected to intensify in coming years, making markets even more dynamic, competitive, and opportunistic. Successful organizations will need to be agile and accelerate their decision-making in an environment where prolonged periods of rapid change will be the new norm. Internal audit will have an opportunity to help management better evaluate its preparedness to deal with future events and the "what if" scenarios that will most likely impact the business. If successful, internal auditors have an opportunity to inform and shape the critical decisions that their management teams must make. The reality is that most professions—internal audit included—are about to go through tremendous change. Many internal audit functions will need to transform themselves to provide foresight and serve in this new capacity. The real question is whether those currently in the profession will recognize the opportunity, prepare themselves, and rise to the occasion or whether the transformation will be led by an influx of new talent who may be viewed as more equipped to embrace change. I suppose it will be a combination of both, and each of us will decide our future to the extent we are willing and prepared to embrace change.

PUNDMANN The No. 1 thing I hear from key internal audit stakeholders—namely, chief financial officers, audit committee chairs, and CEOs—is they need new chief audit executives (CAEs) to come into their roles ready to not only provide assurance, but also to advise and anticipate risks. Internal audit must be proactive. That said, assurance activities are critical, and we're seeing more capabilities like automated assurance help internal audit do block-and-tackle analyses of control effectiveness. Taking those learnings, analyzing them, and using them to identify risks before things actually happen is what sets standout, forward-thinking internal auditors and CAEs apart from the rest.

How can providing foresight help the organization compete?

PUNDMANN It's important for internal auditors to take what they're seeing from a historical perspective and apply it to the future of the organization. If they can identify an emerging risk or trend early and communicate that insight to stakeholders, they can help the business gain competitive advantage. Whether

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

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

ON THE HORIZON

Pundmann and Stewart say internal audit should be aware of, and ready to address, several emerging risks, including:

- Cybersecurity
- Data and cognitive analytics
- Artificial Intelligence
- Robotic process automation
- Blockchain
- Culture
- Third-party
- The rapidly changing strategies of competitors
- Threats from alternative products and innovative business models
- Generational and social trends
- Climate change
- Geopolitical changes
- Government intervention and regulation
- Competition for investment dollars
- Fierce competition for talent

an organization is launching a new product or service or implementing a new technology system, internal auditors should be involved early to assure appropriate steps are taken, anticipate risks, and advise on controls and processes. Things change so fast—it's important to ensure necessary capabilities and controls are built into major efforts long before launch time, and the organization maintains a regular pulse throughout the planning.

STEWART In the future, the success of an organization may be determined more often by an ability to anticipate change, to make the right decision within a compressed time frame, and to execute ahead of the competition. An ability to quickly contemplate the potential risks and benefits of multiple "what if" scenarios will become key to effective decision-making and execution. Internal audit has an opportunity to transition from its past of monitoring historic transactions and controls through more recent efforts to establish continuous monitoring where errors or deficiencies can be quickly corrected, toward a future of what might be termed predictive monitoring, theoretical monitoring, or simply forward-looking assessments, where outcomes can be anticipated, competing ROIs validated, and changes made proactively to enhance execution and improve outcomes. Those organizations that make the best decisions and execute on those decisions in this new paradigm will have an advantage over their competition.

What can internal auditors do to shift to a focus on foresight?

STEWART Internal audit professionals must become more aware of, and educated on, business trends, disruptive technologies, the movements of competitors, and alternatives and must be able to anticipate forward-looking risks. This will require greater industry perspective, stronger interactions between internal audit and the business, greater leverage of subject-matter experts, and advanced risk identification techniques. Internal audit must shift from the traditional and conventional to being more strategic and focused on what might impede the organization's most important business objectives.

PUNDMANN Technology can help a lot. In the future, most internal audit functions will tap risk sensing, predictive analytics, robotic process automation, cognitive computing, machine learning, and—someday—artificial intelligence to help them look to risks and opportunities on the horizon.

What is the risk if internal audit doesn't provide forward-looking assessments?

PUNDMANN Internal auditors who don't offer forward-looking insights may diminish their relevance and their level of impact and influence within the organization. Internal auditors need to be proactive and anticipatory to help their companies gain and maintain competitive advantage. New technologies can help give internal auditors broader and deeper views into the risks they help manage, helping them deliver both insight and foresight.

STEWART An ability to adequately and quickly contemplate the potential risks, benefits, and capabilities of the organization to achieve its objectives for multiple "what if" future scenarios will become so important in decision-making that a failure to have this foresight will not be an option for most organizations. This will be particularly true for areas deemed to be most critical to the organization's success. Management and audit committees will see value in the objective perspective in forward-looking assessments that internal auditors can provide and will seek to transform internal audit functions so they are capable of providing this foresight. Internal audit functions that fail to make this transition likely will find themselves in a less favorable position in the value chain of their organization, will have to deal with an unfavorable contrast to the more advanced internal audit functions of their peers, likely will see more of their budgets and opportunities repurposed to other functions that can support this need, and may ultimately be deemed obsolete and prime to be replaced. Ia

MENU
Meet Our Bloggers
Richard Chambers: Chambers on the Profession
Mike Jacka: From the Mind of Jacka
Laura Soileau: Solutions by Soileau
Jim Pelletier: Points of View by Pelletier

Featuring

Internal Auditor Blogs

Voices with viewpoints on the profession

In addition to our award-winning publication content, we are proud to feature four thought-provoking blogs written by audit leaders. Each blog explores relevant topics affecting today's internal auditors at every level and area of this vast and varied field.

Chambers on the Profession:
Seasoned Reflections on Relevant Issues

From the Mind of Jacka:
Creative Thinking for Times of Change

Solutions by Soileau:
Advice for Daily Audit Challenges

Points of View by Pelletier:
Insights and Innovations From an Insider

READ ALL OF OUR BLOGS. Visit InternalAuditor.org.

Ia
INTERNAL AUDITOR

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

MARCH 11–13
General Audit Management Conference
Gaylord Texan
Dallas/Ft. Worth

APRIL 29–30
Leadership Academy
Disney's Yacht Club Resort
Orlando

JULY 7–10
International Conference
Anaheim Convention Center
Anaheim, CA

AUG. 12–14
Governance, Risk, & Control Conference
The Diplomat
Fort Lauderdale, FL

SEPT. 16–17
Environmental Health & Safety Exchange
Washington Hilton
Washington, DC

SEPT. 16–17
Financial Services Exchange
Washington Hilton
Washington, DC

SEPT. 18
Women in Internal Audit Leadership
Washington Hilton
Washington, DC

SEPT. 20–22
Internal Audit Education Partnership (IAEP) Exchange
Rosen Centre
Orlando, FL

OCT. 21–23
All Star Conference
MGM Grand
Las Vegas

IIA TRAINING

www.theiia.org/training

NEW Auditing IT Governance
On Demand

FEB. 4–15
CIA Exam Preparation – Part 2: Practice of Internal Auditing
Online

FEB. 12–14
IT General Controls
Online

FEB. 12–15
Seminar Week – Multiple Courses
Phoenix

FEB. 19–28
Fundamentals of IT Auditing
Online

MARCH 5–14
Performing an Effective Quality Assessment
Online

MARCH 6–7
Data Analysis for Internal Auditors
Online

MARCH 18–21
Seminar Week – Multiple Courses
Las Vegas

MARCH 19
Fundamentals of Internal Auditing
Online

APRIL 1–12
CIA Exam Preparation – Part 1: Essentials of Internal Auditing
Online

APRIL 2–5
Seminar Week – Multiple Courses
Orlando

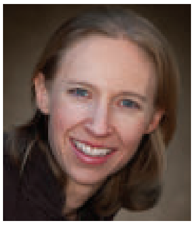
APRIL 2–11
Enterprise Risk Management: A Driver for Organizational Change
Online

BRUARY/MARCH/APR

THE IIA OFFERS many learning opportunities throughout the year. For complete listings visit: www.theiia.org/events

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

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



BY LIZ ORMSBY

THE LOST ART OF CONVERSATION

Auditors need to ensure they're talking to the right people, and having the right kind of discussions.

As auditors, asking questions is our bread and butter. Practitioners are expected to be curious, inquisitive, and even challenging when conducting engagements. But sometimes, despite asking what feels like a million questions, our audits don't progress as we expect or hope. Reflecting on a recent failed attempt to find out what my four-year-old did at day care ("What did you do at day care today darling?" "Nothing, Mummy"), I realized this lack of progression can occur when we aren't asking the right people the right questions—we need a different kind of audit conversation.

Problems can arise initially when conversations take place solely with internal audit's designated client contact—typically the manager in charge of the area being audited. At a previous organization, I led a cash-related audit after my primary contact confirmed the process was critical enough to merit internal audit's attention. But this individual oversaw the process under review—so of course it was considered important. A subsequent meeting with senior management revealed the cash process was a lower audit priority than my team and I originally thought. We could have obtained this information much sooner by holding additional conversations with someone who possessed a more objective point of view.

Even so, identifying the best individuals to speak with does not always guarantee the most relevant information will surface—the discussion itself also requires close attention. Auditors typically prepare questions in advance of client discussions, to make the best use of everyone's time. While the process constitutes best practice, it also presents risks. The auditors may think the meeting is running efficiently as they work through each question, but they could miss the opportunity to explore risks through a more conversational, back-and-forth exchange. If the client simply answers questions with yes or no responses (or "nothing," like my four-year-old), the information gathered may be unhelpful or misleading.

Auditors should occasionally give themselves permission to let the conversation roam and flow. When this happens, some of the topics clients want to discuss inevitably won't conform to the auditors' agenda. Letting the discussion take its course, however, might lead to new insight on what clients view as key risks or opportunities.

In chatting with my four-year-old, I've reconsidered the value of a stock question—asking what train he played with, for example, got a much more detailed response than the standard, "What did you do at day care?" Likewise, a stock question used in audit planning such as, "What keeps you awake at night?" sometimes leads to a useful answer, but often it yields nothing new. Auditors should experiment with different questions, using the audit team's collective wisdom to come up with a variety of possibilities. The right approach to client conversations can significantly enhance internal audit's value, turning a lost art into a productive tool for gathering information. Ia

LIZ ORMSBY, CIA, ACA, CAPM, *is a deputy city auditor at the City Auditor's Office, City of Calgary, Alberta.*

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

An Exclusive
Opportunity