JUNE 2018
A PUBLICATION OF THE IIA

Ia
INTERNAL AUDITOR

#METOO

The movement is shining a spotlight on harassment in the workplace, forcing organizations to recognize the risk and more thoroughly address the issue.

ADVERTISEMENT

Improving Your Professional Brand

In today's internal audit environment, it's all about adding value, and to add value, you must possess knowledge. Learn why Chief Audit Executive Raoul Ménès obtained his Certified Internal Auditor® (CIA®), and why he expects his team to be certified as well.

Certified Internal Auditor®

150,000

What prompted you to become certified?

I pursued certification because I wanted to deepen the knowledge, tools, and techniques necessary to be successful in my day-to-day responsibilities. I was also aware of its power to demonstrate skill, knowledge, proficiency, dedication, and discipline. It validates what I "bring to the table."

How does being IIA-certified set you apart from your non-certified peers?

For an employer, at least on paper, I think it reassures them by validating my qualifications, skillset, and knowledge. It speaks on my behalf. As any recruiter will tell you, if two candidates have similar experience and backgrounds, their preference will always lean towards the certified candidate. As a CAE, I have recently drafted job descriptions for our newly created internal audit activity (based on The IIA's Global Internal Audit Competency Framework) and certification is expected. For team members who are not yet certified, they have one year from their hire date to show progress towards certification.

How has your IIA certification helped your career?

It has provided additional credibility and demonstrated my knowledge in the field of internal auditing. It has also pushed me to deepen my skills and obtain new knowledge due to its continuing professional education requirements. This seems to beg the question: why not pursue certification?

Has earning an IIA certification enhanced your skill level?

Absolutely! The CIA preparation material was not only current and pertinent, it also allowed me to sharpen my "new found" skills and refresh my knowledge of some concepts learned a long time ago! Once certified, I became a stronger, more confident professional that could add more value as one of my organization's trusted and credible audit professionals.

What advice do you have for others who are considering obtaining an IIA certification?

Set an exam date to hold yourself accountable and tell friends and family you are sitting for the exam so that they can motivate and encourage you. Prepare a study calendar that establishes clear deadlines for the various sub-sections, but still allows for the 3Fs: friends, family, and fun! Finally, don't hesitate to reach out to colleagues for assistance.

About the CIA

As the only globally recognized certification for internal auditors and The IIA's flagship credential for more than 40 years, the CIA sets the standard for excellence in the internal audit profession.

Start Your CIA Journey Today.
www.theiia.org/CIA

The Institute of Internal Auditors®

2018-0738

Ia
INTERNAL AUDITOR

JUNE 2018 VOLUME LXXV: III

FEATURES

Ia

INTERNAL AUDITOR

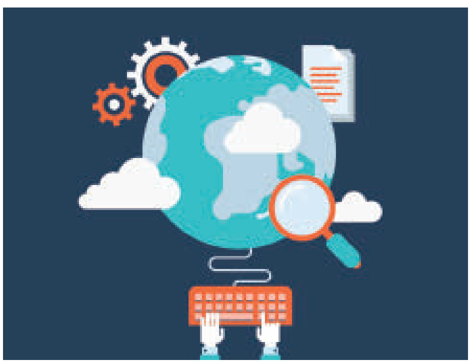
JUNE 2018 VOLUME LXXV: III

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE **InternalAuditor.org**



Audits From Afar Remote audits can leverage technology advances to streamline walkthroughs and free up audit resources.

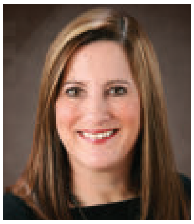
A Boost for Cyber Resilience NIST updates its cybersecurity framework as organizations report mixed results in stopping threats.

Health-care Fraud Is No Accident Insurers, providers, and regulators all have much at stake in fighting false medical billing claims.

Audit Objectivity Watch seasoned audit director Scott Page review a hypothetical scenario and determine whether actions taken violate The IIA's Code of Ethics.

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 © 2018 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.



WHERE HAVE ALL OUR HEROES GONE?

My day ended yesterday with the news that Bill Cosby was found guilty in his sexual assault retrial. Not surprising, but discouraging, as I grew up watching America's dad, Cliff Huxtable. I woke up this morning to the news that yet another iconic television news anchor has been accused of sexual harassment. I used to watch Tom Brokaw every night and have always admired him.

Many of my beliefs from adolescence have been shattered lately, probably because I was taught to respect those in authority. But perhaps the biggest blow to my beliefs was the recent accusations leveled at my alma mater, Michigan State University (MSU). This university has been a huge part of my life. I learned so much from the incredible professors in the School of Journalism. Beyond that, I have two nephews who currently attend the university and numerous family members who went there. My family cheers for MSU and considers its teams our teams, even though we've lived in Florida for nearly 20 years. I have an MSU flag flying outside my house. (You get the picture.)

The Larry Nassar story is beyond horrifying, and it breaks my heart that it happened at MSU. It would be bad enough if the story ended with Nassar, but it doesn't. MSU's former dean of the College of Osteopathic Medicine William Strampel reportedly failed to ensure restrictions were put on Nassar's practice following a 2014 abuse complaint and now faces charges of sexual misconduct, himself. After this and more came to light, I had hope that MSU's interim president, John Engler, would enact the changes necessary to make MSU whole again. However, he's now being criticized for his response to survivors and there are calls for him to step down.

As this Editor's Note was going into production, the *Detroit Free Press* reported that MSU had settled lawsuits with all 332 victims of Nassar's assaults at a cost of nearly $500 million. Finally, some good news. The *Free Press* published a statement from the MSU Board: "We recognize the need for change on our campus and in our community around sexual assault awareness and prevention."

It's satisfying to see the women who have suffered sexual assault and harassment finally coming forward and getting restitution. The #MeToo movement (read "Into the Light," page 20) is forcing organizations, and internal audit, to take a closer look at sexual abuse and misconduct and how it is investigated and addressed.

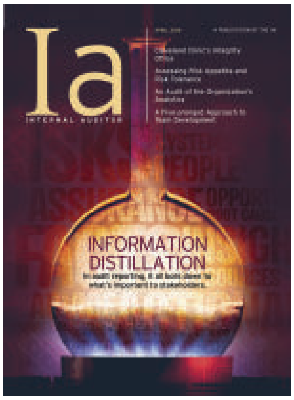
Where have all our heroes gone? They're still here. They are the women who are stepping forward and fighting back. And, they are the men and women in our organizations who are listening and addressing these issues.

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.



To the Point

I agree that internal audit reports should be sharp enough to pinpoint the actual problem with root causes. Our risk-based audit reports take note of the above and give all the findings on one sheet in an executive summary.

RAVI PRAKASH *comments on Norman Marks' "Information Distillation" (April 2018).*

The Written Message

Anne Millage provides great points for auditors to use in written communication to stakeholders. It amazes me how auditors forget that their audience is someone not familiar with their work. In my experience, auditors sound like they are writing to a college professor or act like an elitist with fancy words. However, this mentality hides the important parts of your written message. Keep it short, simple, and to the point, or risk being ignored.

FREDRICK W. LEE *comments on Anne Millage's "Words Matter" ("Editor's Note," April 2018).*

Worker Safety

Only after reading Tom O'Reilly's article did it dawn on me that companies/agencies should evaluate, as he put it, "enterprise risks to worker safety and well-being." Especially working for an agency whose primary mission is to serve and protect, I firmly believe that the internal audit function should look at ways to reduce risks for the sake of the very lives of the officers who are often in harm's way.

JAMES KIM *comments on Tom O'Reilly's "Protecting Employees" ("Risk Watch," April 2018).*

The Future of Internal Auditing

We need to expand our recruiting beyond the traditional accounting and finance professionals. If you are recruiting at universities for interns or entry level auditors, there are many other business and IT-related majors that would also add value such as international business, data analytics, business information systems, and supply chain management. Depending on your industry, there are many more that can bring a different, but important, perspective to the department.

FRANK HOLLOMAN *comments on the Chambers on the Profession blog post, "What Will Internal Audit's Future Leaders Look Like?" (InternalAuditor.org).*

Capacity for Creativity

I don't think it's too late, nor do I believe internal audit lacks creativity. Some individuals surely do, but as people, we have a full spectrum of ability and capacity for creativity and innovation. The distribution curve is probably shaped like a bell. One of the things I love about auditing is the need to continuously research, learn, and share—whether it's about fraud schemes, new analytics techniques, new processes our organizations are implementing, new technologies ... we cannot provide the assurance we need if we don't understand the threats and opportunities to the business. We learn or perish.

RICK FOWLER *comments on the From the Mind of Jacka blog post, "It May Be Too Late for Innovation" (InternalAuditor.org).*

Ia
INTERNAL AUDITOR
JUNE 2018
VOLUME LXXV:III

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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


Are you prepared?
Public Sector Virtual Symposium
July 24, 2018 | 10 a.m.–2 p.m. | Earn 4 CPE Credits
This premier online training opportunity, Preparing Public Sector Auditors for Tomorrow's Terrain, provides government auditors a chance to learn and engage through a convenient and flexible web-based console. Join four dynamic speakers as they discuss the challenges and opportunities unique to government auditors and the public sector arena.
Register Today
at www.theiia.org/VirtualSymposium
The Institute of Internal Auditors
Public Sector™
AUDIT CENTER
2018-0653

Culture's impact on performance... Fraud isn't reported to the police... Setting the tone against harassment... Engaging auditors in transformation.

Update

DOING THE RIGHT THING

Last year, nearly 70 percent of employees who observed misconduct in the workplace reported it.

70% Sexual harassment

Failed specifications **73%**

76% Bribes or kickbacks

Misuse of confidential information **79%**

74% Theft

Source: Ethics & Compliance Initiative, 2018 Global Business Ethics Survey

FACING RISK HEAD-ON

Corporate concern drops for economic and political surprises.

Companies are adapting to new economic realities and appear more comfortable with uncertainty, according to the 2018 Global Business & Spending Outlook. The survey, conducted by American Express and Institutional Investor Thought Leadership Studio, finds that companies have substituted a fear-based, reactionary response to risk with "a more tempered managerial approach." The proportion of respondents who agree that widely unanticipated events are a rapidly growing concern at their companies dropped from more than 90 percent in 2017 to 64 percent this year.

Increasingly, companies are facing risks from economic and political uncertainty head-on. Far fewer (59 percent) of the 870 financial executives surveyed say they anticipate withdrawing business from high-risk geographic areas. In 2017, 87 percent said they planned to move business from such regions.

Rather than retreating from risk, almost 70 percent of companies indicate growing interest in expanding enterprise risk management programs, compared to 43 percent in 2017. More than half express interest in asset-protection initiatives.

"For large and global companies, uncertainty has become the new normal," says

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

IMAGES: TOP: ESB PROFESSIONAL / SHUTTERSTOCK.COM; LEFT, PHOTO MELON / SHUTTERSTOCK.COM

Brendan Walsh, executive vice president, American Express Global Commercial Services. "As they pursue sustained gradual growth, the leaders of these firms are taking a back-to-basics approach and focusing on the fundamentals—better serving customers, developing new products, entering new markets, and prioritizing business transformation and innovation."

Although anxiety over economic, political, and environmental disruption has diminished, organizations remain vigilant, and their spending plans indicate greater risk mitigation, according to the survey. This year, uncertainty over economic and political issues is affecting organizations' spending almost equally inside and outside the respondents' countries.

In 2017, economic and political uncertainty outside respondents' countries was twice as likely (nearly 75 percent) as domestic ambiguity (36 percent) to prompt greater caution over spending and investment.

– D. SALIERNO

THE HIGH COST OF POOR CULTURE

Bad workplace culture is affecting business performance.

Poor company culture costs U.K. businesses $32 billion (£23.6 billion) per year, according to The Culture Economy, a report from U.K.-based human resources software company breatheHR. Moreover, dissatisfaction with workplace culture leads one-third of surveyed British employees to quit their jobs.

Despite this, 60 percent of small and medium-sized enterprise (SMEs) leaders surveyed consider company culture as a "nice to have." Culture has a clear impact not just on business success, but on the economy and our society," says breatheHR CEO Jonathan Richards.

One area affecting workplace culture: employee distrust in senior management. This is because employees don't feel supported by management (59 percent), don't think management knows what it is doing (53 percent), and say management is not transparent (45 percent).

– S. STEFFEE

70%

OF ENERGY SECTOR IT SECURITY PROFESSIONALS are concerned that a successful cyberattack at an oil and gas company could result in catastrophic failure.

56%

AT COMPANIES THAT HAVEN'T INVESTED IN INDUSTRIAL CONTROL SYSTEMS SECURITY say it would take a significant attack to get their company to do so.

"It's concerning that more than half would wait for an attack to happen before investing properly, given what's at stake with critical infrastructure," says Tim Erlin, vice president of product management and strategy at Tripwire.

Source: Tripwire and Dimensional Research, ICS Security in the Energy Industry

FAILURE TO PROSECUTE

More organizations don't report fraud incidents to authorities.

Organizations continue to suffer losses from occupational fraud, but fewer are reporting it to law enforcement, according to the 2018 Report to the Nations on Occupational Fraud and Abuse. The biennial report from the Association of Certified Fraud Examiners (ACFE) notes that the median loss from a fraud incident investigated by certified fraud examiners in the past two years is $130,000. Twenty-two percent of losses exceeded $1 million.

Yet, organizations reported just 58 percent of cases to law enforcement during this period, continuing a decline since the 2008 report when the rate was 69 percent. Organizations cite fear of bad publicity (38 percent), internal discipline being sufficient

IMAGES: TOP, ALEXWHITE / SHUTTERSTOCK.COM; RIGHT, PHOTOGRAPHEE.EU / SHUTTERSTOCK.COM

(33 percent), and cost (24 percent) as reasons for not reporting incidents to law enforcement.

Opting not to prosecute cases can have negative consequences, says John Warren, vice president and general counsel for Austin, Texas-based ACFE. "This enables [fraudsters] in many cases to move on to other employers and repeat their crimes," he explains.

Small businesses have it worse than large organizations, with median losses of $200,000, the report says. Small organizations face different risks than large counterparts—billing (29 percent), check and payment tampering (22 percent), expense reimbursement (21 percent), and skimming (20 percent). Moreover, they have fewer anti-fraud controls.

Conversely, large organizations have "a greater ability to separate duties among staff members to prevent fraud," the study notes. Size has a downside, though. "The large staff size can also mean more potentially dishonest employees who might attempt schemes and more complex processes and transactions, which can increase the risk of fraud," the report points out.

As with past studies, tips are the most common fraud detection method (40 percent), followed by internal audit (15 percent) and management reviews (13 percent). Having a hotline greatly increases the percentage of cases detected by tips. **—T. MCCOLLUM**

SET A GOOD EXAMPLE

When it comes to harassment, employees are watching, says Wendy Sellers, chief operating officer of business consulting firm BlackRain Partners.

How can organizations demonstrate to their employees that sexual harassment is a top priority? Harassment is a form of discrimination. Educating your entire team on how to be inclusive is vital. The company's written policy should clearly outline how and to whom an employee can report harassment. It should be clear that the company is willing to end relationships with vendors, contractors, and customers who commit harassment against its employees. Finally, all supervisors should be trained yearly on inclusivity, harassment, and discrimination. It is fundamental that executive leadership is engaged in this training. Employees are watching and will follow by example.

When faced with a sexual harassment accusation, an investigation must be started within one business day of the report. Have a professional, respectful investigation plan—and possibly a media plan—ready to go. Remember to stick to the facts while using empathy. Be transparent to those involved while remaining confidential. Termination is the only solution for severe harassers or supervisors who are guilty of harassment.

DIGITIZATION CHALLENGES IT AUDITORS

Technology specialists need to engage with transformation projects.

IT audit specialists must step up their games to deal with the new risks posed by transformation efforts, according to the latest IT Audit Benchmarking Survey from ISACA and Protiviti. IT auditors need to collaborate more with IT and other business functions and engage more in technology projects, the report states. Indeed, technology specialists should be involved throughout the project life cycle "to ensure policies and processes are put in place to mitigate risk," says ISACA Chairman Theresa Grafenstine.

Cybersecurity and privacy are the top concerns of the more than 1,300 chief audit executives, internal auditors, and IT audit vice presidents and directors who responded. Those concerns are shaping audit plans, as well, as organizations seek to protect data from new threats and address regulations such as the European Union's General Data Protection Regulation.

Digitization creates new opportunities to mine data for business insights, but "it also adds significant risk and therefore data protection needs to be prioritized," says Andrew Struthers-Kennedy, global leader of Protiviti's IT Audit practice.
—T. MCCOLLUM

PHOTO: LEFT, NMEDIA / SHUTTERSTOCK.COM

Back to Basics

BY CHRISTINE HOGAN HAYES EDITED BY JAMES ROTH + WADE CASSELS

CENTRALIZED VS. DECENTRALIZED AUDIT FUNCTIONS

CAEs should weigh the advantages and disadvantages of each structure when considering the best organizational fit.

Internal audit departments typically are structured as centralized or decentralized. Department structure plays an influential role within the department, as well as in the business operations that are audited. Therefore, it is crucial for internal audit management to evaluate which structure is the best fit for its team and the business.

Per The IIA's International Professional Practices Framework, an organization's internal audit activity is required to be in conformance with the *Standards*. However, the *Standards* do not specifically address departmental structure, so the chief audit executive (CAE) can determine how the internal audit activity is set up by examining the advantages and disadvantages of both centralized and decentralized.

Centralized Structure

In a centralized audit department, management and staff work in the same location and either travel to other office locations or work remotely to conduct audits. The centralized structure offers many advantages. First, internal audit leadership works in the same office. Members of management—ranging from supervising seniors to the CAE—not only meet in-person, but, more importantly, demonstrate a consistent "tone at the top." Also, with the entire team in the same location, any team member has access to management, which can encourage informal, in-person coaching and mentorship.

Having the team together also promotes consistency in training, both at the entry level and experienced practitioner level. Internal audit policies and procedures, such as workpaper expectations, can be communicated and compliance monitored with greater uniformity. As it relates to uniformity, a centralized department can promote more equal opportunities, such as audit project assignment. In addition, when all staff work out of the same office, more collaboration among team members can occur.

There also are disadvantages with a centralized departmental structure, such as the inevitable travel component to the job—especially at the staff and senior staff levels. For some, the opportunity to travel the world may be appealing; however, because the time spent on the road can be extensive, it may be difficult to attract and retain top talent. Although conducting audits remotely can decrease the travel commitment, there are some audits that still require on-site walkthroughs; detailed test work; and meetings that cannot be performed via email, phone, or teleconference. On-site audit fieldwork activities are valuable, as there is much to gain when working with the audit client in person. This can be

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

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

a benefit not only in the current audit, but through observation and informal meetings, candid conversation about the site's operations can highlight what's really going on. Additionally, there is value gained when internal audit is geographically closer to the operations it audits, as continual dialogue about regional policies and practices can assist internal audit during its risk assessment and audit planning processes.

Decentralized Structure

A decentralized department assigns internal audit teams in more than one location, and each team is responsible for auditing that office's (or region's) operations. The decentralized internal audit department also offers many advantages. First, when audits are performed at a more local level, there is increased opportunity for internal audit staff members and management to collaborate throughout the actual audits. Internal audit managers can coach employees and provide advice in a variety of areas, such as walkthrough and interview techniques and workpaper and documentation execution. Unlike the centralized structure, where managers might supervise the team remotely, staff members benefit from the in-person guidance when managers are available on-site.

Additionally, with a decentralized model, audit staff members and management are close to the business operations under review, which can help forge relationships that result in candid dialogue about risk and controls. This can prompt requests for consulting engagements and advisory reviews, which benefit both internal audit and management.

There also can be some drawbacks to using a decentralized model. First, staff members (and management) may develop expertise limited to the office and region where they work. For example, auditors can gain expertise about part of a process that occurs in their location, such as product design, but miss other process components, such as manufacturing, that help complete the full picture of the process. Specialization also can limit skill development.

Another downside to a decentralized department is that each auditor typically performs multiple audits at the same time. Unlike a centralized model, which often can incorporate travel (and therefore, each auditor is assigned one project at a time), a decentralized model assigns multiple audit projects to each auditor, which can cause scheduling problems and demand careful attention to balancing priorities and deadlines.

> **It is critical to assess how internal audit's structure aligns with the organization.**

Organizational Impact

Once internal audit leaders weigh the structure's impact on the department, itself, it is critical to assess how the structure aligns with the organization. Two perspectives that can be used to evaluate organizational impact are company culture and structural alignment.

Company culture is the organization's overall environment and atmosphere. It comprises the stated policies and procedures, as well as the values and norms, both of which permeate interactions, communications, and expectations. Every culture is different, as each organization has its own history and experiences that uniquely shape how the organization makes decisions. Internal audit leaders, therefore, need to determine how the selected department structure will complement the company culture. For instance, if the overall culture encourages manager/employee collaboration as a method to effectively support and train emerging talent, then a decentralized audit department may be a good fit. Such a structure enables managers to be on-site during audits and provide in-person feedback and coaching. However, a different company may encourage a talent development model that promotes professionals as generalists (as opposed to specialists), and therefore, a centralized audit department, which permits a wider range of audit project opportunities, may be a better choice to achieve congruence with the overall culture.

The manner in which other departments are structured within the organization influences the audit department's structure. Does the organization have satellite locations? If so, what departments reside in those offices? If there are minimal resources in other offices, then a centralized audit department structure may be a best fit. However, if the organization is experiencing rapid growth in a certain region, an internal audit leader may consider a decentralized structure; by placing dedicated resources in that region, internal audit can partner with local management and collaborate on evaluating key risks and controls.

Thoughts for the Future

The determination of an internal audit department structure that supports both the audit team and the organization is an important decision made by the CAE and internal audit management. Like many other management decisions, it is worthwhile to evaluate the structure's continued relevance and applicability periodically, as organizations change—sometimes extensively—over time. ia

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

ITAudit

BY CLIFF DONATHAN EDITED BY STEVE MAR

PARTNERS IN PROTECTION

Now more than ever, internal auditors and information security officers need to collaborate on cybersecurity.

Despite organizations increasing cybersecurity spending by 23 percent last year, successful security breaches rose 27 percent compared to 2016, according to the 2017 Cost of Cyber Crime Study. The joint study by Accenture and the Ponemon Institute is based on interviews with more than 2,100 cybersecurity and IT professionals worldwide. To find out what went wrong, researchers looked at the value organizations gained from nine areas of cybersecurity investments. What they discovered is that organizations are investing in the wrong areas when it comes to cybersecurity and risk.

Take perimeter security, for example. Advanced perimeter controls are the highest spending category, while being fifth in cost savings. Yet, focusing primarily on perimeter security makes less sense when most companies can't even define their perimeter in the age of the Internet of Things. Research firm Gartner predicts there will be 20 billion internet-connected devices by 2020, up from 6 billion devices in 2014.

As the areas where attackers can target continue to expand, organizations need their cybersecurity and internal audit functions to partner to more effectively deploy resources against cyber threats. Cybersecurity teams and executive management can leverage internal audit's insight into organizational risks to invest in areas that can provide the greatest protective and efficiency value to the business. To build this relationship, both internal audit and cybersecurity professionals will need to change how they do business and collaborate to build cybersecurity and risk management strategies and inform executive management.

Hiding Flaws

Neither cybersecurity professionals nor internal auditors are wholly innocent when it comes to how they work together. Too often, cybersecurity teams are defensive when it comes to internal audit. They don't want to look bad in front of their peers and management, so they try to conceal their flaws from auditors. At best, this produces a strained relationship between internal audit and cybersecurity, and at worst, it exposes the business to vulnerabilities and threats.

Executive management needs clear information about the risks so it can make the best decisions on where to spend resources to enable the business to operate securely. Internal auditors can help cybersecurity professionals provide this information by giving them a second pair of eyes to find security flaws before a malicious user might exploit them. In addition, a strong relationship with auditors can provide the cybersecurity team a broad view of the organization and its risks. Otherwise, the cybersecurity

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

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

team can lose sight of the organization's overall risks as it concentrates to protect the business' systems and assets. Finally, with its access to executive management and the board of directors, internal audit can communicate the severity of risks and their impact to the business when the cybersecurity team cannot get the appropriate visibility.

Ignoring Cybersecurity Plans

Internal auditors share blame, too. Often, auditors are quick to make independent assessments outside of the cybersecurity team's plans, which can lead to inappropriate prioritization of risks. Consider this example:

> Bill performs an IT security audit of his business. While planning his audit, he researches the generally accepted frameworks, best practices, and the company's IT security policies. Bill does not consider the cybersecurity team's roadmap or plans, which show that the team's No. 1 priority is to shore up the business' asset management program.
>
> During the fieldwork, Bill finds that not all systems have the appropriate security agents installed on them. He reports his finding and a management action plan and date are set. Because the company takes internal audit seriously, that action plan takes priority over the cybersecurity team's roadmap.

The problem with this scenario is that if the cybersecurity team is forced to concentrate on agent deployment, it can't shore up its asset management. That can lead to future issues with agent deployment because the business lacks a clear understanding of its hardware and software assets. Without a clear partnership between internal audit and cybersecurity, the business may overspend and under protect its assets.

Internal audit, itself, stands to benefit from partnering with the cybersecurity team. Cybersecurity professionals can become deep experts in their field and have access to the latest research from security-focused professional associations. They can give auditors a better understanding of current and upcoming threats to the business and how they interplay with other business risks.

Auditors also can benefit from learning how the tools and strategies the cybersecurity team has deployed work with each other to build defense in depth. Often, auditors may have a single understanding of how a certain set of controls should be implemented to protect an area of the business. For example, developer access to production historically has been considered a security issue that must be addressed, with clearly defined lines of segregation of duties needed. However, DevOps and continuous release change management are blurring the lines of traditional segregation of duties risks. Today, small, agile teams rapidly create, test, and auto-deploy application code. This would be impossible in traditional segregation-of-duties-based development life cycles. Partnering with the cybersecurity team will help auditors understand the risks this new way of working brings to the business.

Team Building

A successful collaboration between cybersecurity and internal audit requires two essential ingredients: communication and empathy. Communication should happen at least monthly, and the two functions should conduct a full agenda focused on risk management and cybersecurity threats and plans at least quarterly. The other meetings can be less formal with some emphasis on getting to know people to cultivate empathy.

Empathy is about walking in someone else's shoes. There is no better way to do that than to actually do that person's job. Cross-training employees can help an organization be successful. Because internal audit and cybersecurity have a common concern with risk management, they are a natural fit for job rotations between them.

A successful collaboration requires communication and empathy.

Another way to build empathy is to have internal audit and cybersecurity team members pair up to present training sessions at events such as in-house lunch and learns and local conferences. Finally, the two teams can partner to perform the organization's cyber risk assessments.

A Symbiotic Relationship

Ultimately, the key byproduct of internal audit's partnership with the cybersecurity team will be to give management and the board a clear understanding of the cyber risks and opportunities the business faces. That information can enable them to make the best decisions about which security tools to invest in and how and where to deploy those resources. This can't happen without a symbiotic relationship between auditors and cybersecurity professionals. By gaining a deeper view into the organization's security risks, internal audit can produce a global assessment of cyber risks and leverage its relationships with executive management and the audit committee to drive effective change to protect the organization. Ia

CLIFF DONATHAN, CISA, CISSP, CCSK, *is senior director of Information Security at Experian Health in Franklin, Tenn.*

Fraud Findings

BY JOHN NEY + JESSICA SMITH EDITED BY BRYANT RICHARDS

THE CFO CHECK SCAM

A routine internal audit uncovers a $1 million fraud carried out by the company's former chief financial officer.

Assigned to what appeared to be a routine audit, internal auditors Juan Morales and Jim Burton were sent to the Ottawa office of Smith Construction Inc. (SCI), an engineering and construction subsidiary whose parent company, U.S. Constructors Inc. (USCI), was headquartered in New Jersey. SCI made most of its profits from manufacturing boilers and associated products for electric power generation plants and oil and gas refineries. Generating approximately $200 million in annual sales, SCI was in good standing with USCI. However, it began to struggle when senior management at USCI started implementing highly aggressive sales targets. Once sales numbers could not keep up with anticipated goals, SCI began to spiral toward disaster.

SCI was faced with significant charges against earnings based on poor business decisions that led to several cutbacks and layoffs at the Canadian operations. Employees responsible for managing the vendor master file—a list of all the company's suppliers—were laid off as a cost-cutting measure and the accounting department was reduced from seven to four people. The aggressive layoffs inevitably led to a potential lack of segregation of duties. A task or process previously performed and reviewed by several people became the responsibility of one individual. In many cases, the responsibility fell to the company's chief financial officer (CFO), Paul Fournier.

After a few more significant charges against earnings, senior management terminated Fournier and the business unit CEO. Per company policy, every time a high-level employee left the company, internal auditors were assigned to check the critical general ledger accounts, including cash. Burton's position was his first audit job after working in the accounting field for just under one year. Due to his lack of experience, Morales, his supervisor, assigned him to look over the company's liability accounts, which included accounts payable and accruals, as it was considered the most routine part of internal auditing.

Reviewing the details of the company's liabilities requires a simple, step-by-step process that even an inexperienced auditor could perform. By following each step of standard internal audit procedures, Burton was able to uncover an enormous fluctuation in liabilities. He noticed that around $30,000 was being made payable every month to a law firm in Boston. He mentioned this to Morales and the two decided to look into it further. An engineering and

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

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

LESSONS LEARNED

- » Segregation of duties is crucial for every company and is the easiest way to prevent fraud from occurring. Even when faced with major cutbacks, it is important to make sure duties within the accounting department are performed and reviewed by different personnel. This internal control separates key processes to make fraud more difficult to attempt.
- » Companies should always keep an updated vendor master file. The process of updating it should go through several employees to ensure accuracy and prevent fraudulent payments to fictitious vendors. Employees responsible for issuing payments should never be able to modify the vendor master file.
- » Employing internal audit after a high-level employee leaves the company is a good practice and should be the case for all companies. A post-departure audit review helps companies catch fraud that may have otherwise gone completely undetected and prevent new hires from getting involved in the actions of the previous employee in their position.
- » A strong and trusted audit program with clearly documented procedures can help even a rookie auditor discover fraud. Though this will not guarantee that a fraud will be detected, even if procedures are followed with due care, internal auditors can be a deterrent for employees looking to commit fraud.

construction company making regular payments in significant amounts to a law firm outside of the country was suspicious. They discovered that the law firm specialized in international trade issues related to the North American Free Trade Agreement (NAFTA), but it had been several years since the company required legal expertise related to NAFTA issues. This fact prompted them to look into the situation even further. Morales contacted the law firm and asked to speak to the accounting manager, who revealed that SCI had not been an active client for four years and there was no record of the company in their accounts receivables records. Burton also found a check made out for $12,000 to the law firm that had not been cashed for two months, which created more suspicion.

Most checks were signed "for deposit only" and written by hand.

Because the review had occurred before any sort of electronic records existed, Burton and Morales had to retrieve physical canceled checks from boxes in the record storage area of the basement to see who had endorsed them. They found most checks were signed "for deposit only" and written by hand instead of stamped with the company's name. After hours of going through boxes, they found a check endorsed with Fournier's signature. When they pulled the vendor master file, they realized that check payments to the law firm were being sent to an address in Canada, not the U.S.

After the layoffs, Fournier became the only one in charge of the vendor master file and was able to change data with no other type of review. This allowed Fournier to manipulate the information on the vendor master file on his own, without co-workers noticing. He changed the firm's address to one in Canada so he would be able to cash the checks on his own behalf. He copied and pasted data from legitimate invoices from the law firm, presented them for payment, noted them in the accounting records, and filed them.

Realizing this case could require third-party expertise, Morales and Burton called the CAE and controller at USCI to recommend a forensic investigation. The forensic investigators recreated all of the accounting books to reveal what they should look like and exactly how much was missing. Ultimately, this effort revealed a total of $1.1 million in checks from the U.S. cashed in Canada over three years. Morales and Burton remained on site assisting with procedures such as cash reconciliation and overhead analysis. Based on recommendations from USCI's general counsel and outside counsel, Fournier was issued a Form 1099 that recorded the $1.1 million he had stolen from the Canadian subsidiary and notified the U.S. Internal Revenue Service of his compensation received through the fraud. Fournier was eventually convicted of the fraud and sentenced to a U.S. federal prison for 18 months. Ia

JOHN NEY, CPA, *is senior manager of compliance at L3Technologies in Rockwall, Texas.*

JESSICA SMITH *is an accounting major at Nichols College in Dudley, Mass.*

MEDIAPHOTOS / ISTOCK.COM

When the dust settles, disgraced movie mogul Harvey Weinstein may actually end up helping women in the workplace. More than 85 women have come forward with their stories of sexual harassment and sexual assault at the hands of Weinstein, including retaliation in the form of blacklisting them from acting jobs for rejecting his advances.

The Weinstein scandal has become a social media firestorm that has propelled a movement — #MeToo — thousands of tweets, Instagram posts, and press conference comments, raising the profile of sexual harassment on legislative agendas and in corporate boardrooms. Publicity around the topic is drawing attention to the risks harassment represents and the processes companies implement to manage those risks — areas where internal auditors are key players in their organizations' harassment prevention and mitigation efforts.

A SHIFT IN RESPONSE

Is the definition of *sexual harassment* changing? Betty McPhilimy, retired chief audit executive (CAE) at Northwestern University in Evanston, Ill., says no. Rather, "clarity is setting in." Personal workplace priorities haven't changed, either, she adds: "Everyone wants to be treated with respect."

Brian Koegle, a partner in the employment and labor law department of the Los Angeles office of Poole & Shaffery LLP, agrees. "Legally speaking, the definition of *harassment* in the workplace has not changed," he says. "It does evolve, but there have been no material changes to the definition or

INTO

#MeToo is shining a light on the harassment women have faced in the workplace for decades and have been afraid to report.

the light

Russell A. Jackson

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

to how it's interpreted under federal or state law for the better part of 15 years."

What's recently changed is the mix. "From the late 1980s until about 10 months ago, the most prevalent legal claims involved harassers creating hostile work environments," Koegle says. "But now the overt, obscene cases are coming up more frequently, which we hadn't seen for years until the Weinstein scandal broke." He attributes this to the empowerment movement the scandal has spawned, where "women are feeling strong enough to come forward and say what's actually happening after decades of fearing being blackballed." The change, he adds, is especially evident in Hollywood, where there's a groundswell of support. "It's a social norm shift, rather than a legal shift."

"Corporate response is changing, with more attention and responsibility focused on harassment issues and policies," says Bettina Deynes, chief human resources officer at the Society for Human Resource Management, in Alexandria, Va. "The acceptance of primary responsibility for policy and enforcement by management is also increasing." Human resources, she adds, must "create and publish policies that are clear and effective and that have strict penalties for unacceptable behavior." It also must be simpler and less intimidating to report incidents of sexual harassment. "It's a necessity," she stresses, because "the risks of sexual harassment—lawsuits, internal conflicts, and employee terminations—are increasing."

CASES ARE CLIMBING

While the U.S. Equal Employment Opportunity Commission (EEOC) has not reported a surge in the number of harassment claims, Koegle says that it's been exactly the opposite. "We've conducted more workplace investigations in the last four months than in the last five years, and we're seeing more written in journals on harassment," he says. There may be an explanation for the EEOC's numbers, according to Robin Shea, an attorney with the Encino, Calif., firm Constangy Brooks Smith & Prophete LLP. In a blog post, Shea says the EEOC reporting period ended Sept. 30, before #MeToo gained prominence. "Brace yourself for 2018," she says in the blog. "Retaliation was the most common claim in 2017, and prelitigation monetary relief in harassment charges was at its highest since 2010."

As women read more #MeToo stories, some may realize that an incident in their past—that at the time they felt was inappropriate—was, in fact, sexual harassment. Social media is causing the estimated 85 percent to 95 percent of women who don't report the incident when it happens to reflect and come forward with their own stories. "I look back and I'm dumbfounded that I didn't leave or tell someone," says Tori Reid, a West Hollywood, Calif.-based actress, writer, and producer who grew up in a show business family. "I didn't have kids to raise. I wasn't desperate to keep the job. I guess I didn't realize it was harassment. On a certain level, in the back of your mind, it's the way we've known the entertainment workplace to be." She avoided the worst of it. "Sixty percent of the work was making sure my boss didn't put his hands on me," she says. "I was dodging and ducking." This year, she participated in the #MeToo unity demonstration at the Golden Globe Awards.

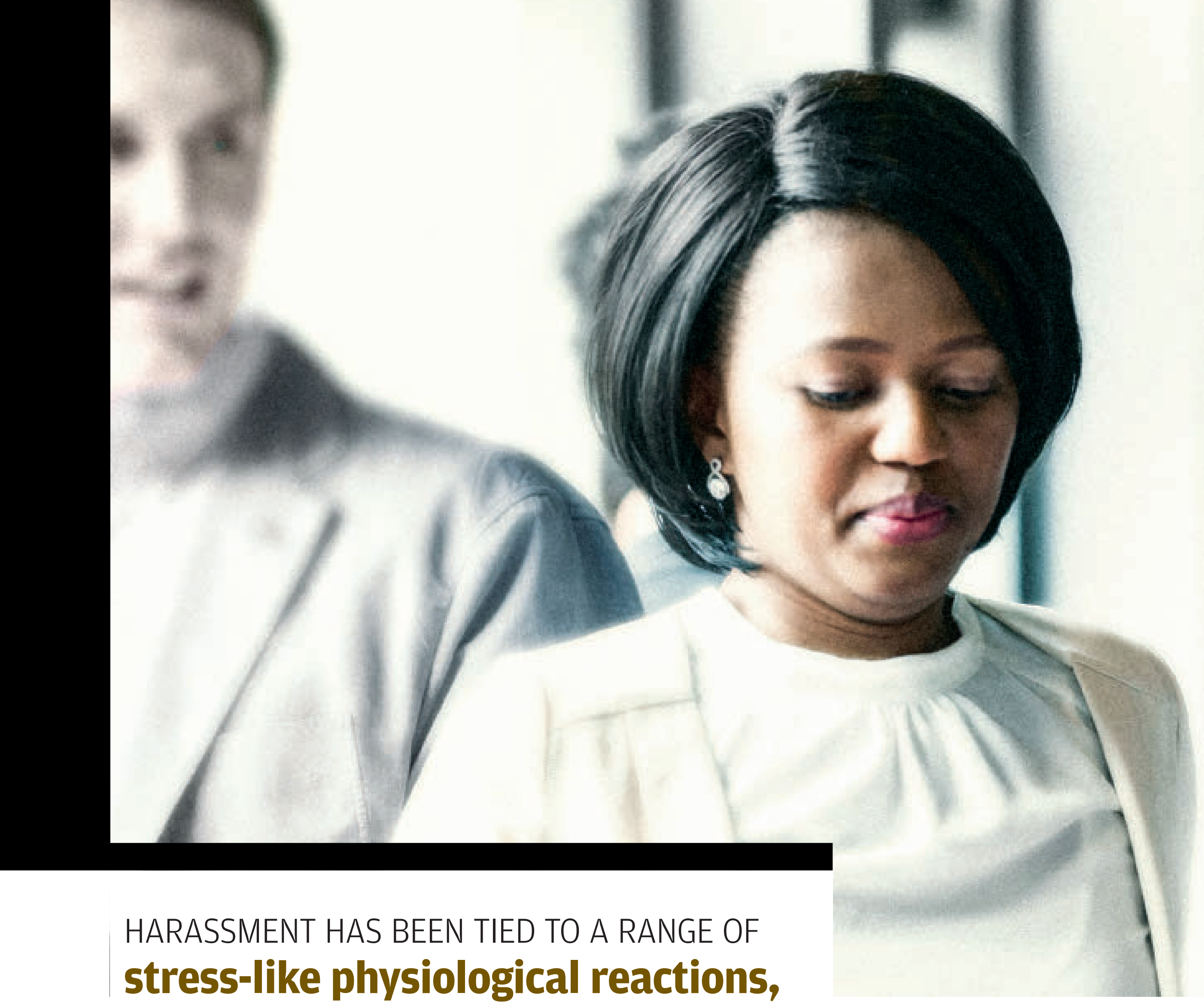
Harassment victims have testified about "slaps on the butt, repeated comments about breast size, and requests for sex," a *Kaiser Health News* report found. And men are victims, too. A 1998 U.S. Supreme Court ruling in Oncale v. Sundowner Offshore Services Inc. said same-sex harassment of both sexes is actionable, and juries have held women responsible for harassing men.

WHAT'S AT RISK

Regardless of gender, this behavior has "a cumulative long-term negative impact on performance," says Ed Lynch, assistant professor in the Department of Accounting at California State University at Fullerton's Mihaylo College of Business and Economics. According to the Washington, D.C.-based National Women's Law Center (NWLC), "victims suffer profound economic and emotional harm"—and its physical manifestations. Up to 70 percent of women and 45 percent of men have experienced harassment, University of Maine sociologist Amy Blackstone recently told livescience.com. Many victims feel self-doubt that turns into self-blame, which then turns into depression—and, for some women, post-traumatic stress disorder. Harassment has been tied

HISTORY OF #METOO

Corporations addressing the risks represented by sexual harassment can thank civil rights activist Tarana Burke for spurring the improvements they're making. She first used "Me, Too" in 2006 as shorthand for efforts to unify behind changing the harassment paradigm. In 2017, she was among the "Silence Breakers" *Time* named as "Person of the Year." Actress Alyssa Milano took a friend's advice to flood Twitter with the phrase, urging women who've been harassed or assaulted to retweet the two words. Her effort generated more than 200,000 responses in 24 hours. It became a top topic on Facebook, and Time's Up, a defense fund and pressure group, formed to keep the message moving.



GCSHUTTER / ISTOCK.COM

HARASSMENT HAS BEEN TIED TO A RANGE OF **stress-like physiological reactions,** INCLUDING SLEEP DISTURBANCES, NECK PAIN, AND INCREASED RISK OF CARDIOVASCULAR DISEASE.

to a range of stress-like physiological reactions, including sleep disturbances, neck pain, increased risk of cardiovascular disease, and, in extreme cases, increased risk of suicide.

The primary effects can destroy economic and career well-being. *The New York Times* examined the damage that fear of harassment allegations can cause to mentor-like relationships young executives develop with senior leaders. "All too often, we wind up prosecuting the victim as much as the alleged harasser," Koegle points out, "with all the gossip and innuendo that can surround workplace harassment allegations." One of the most important elements of an investigation, he says, is "making sure victims feel the company is supporting them, that someone's got their back, and that nothing happens to them that's retaliatory."

There should be greater transparency in complaint handling, Lynch says, including how companies develop codes of conduct and related training and how they craft policies for follow up. He argues that transparency "enables the identification of prevention best practices" and outweighs any risk of reputation damage, which actually acts as an incentive for change.

EMPLOYERS' RISKS RISING, TOO

In fact, organizations risk image damage anyway. "The primary risk is reputation," says Robert Kuling, a partner in Enterprise Risk Services at Deloitte Canada in Calgary. "Getting into the public domain with issues around discrimination and harassment can absolutely destroy a company's brand and trust." For example:

- Weinstein's studio has filed for bankruptcy, CNN reports, and terminated all confidentiality agreements that have kept more people from coming forward. Lantern Capital Partners agreed to acquire the studio after a separate deal to sell the assets fell apart.
- The CBC News website reported that Toronto's Soulpepper Theatre Co. lost $375,000 in planned federal funding after its artistic director, who resigned, was accused of sexual misconduct and harassment by four actresses. The women are suing for $4.25 million in damages from Soulpepper and $3.6 million from the executive. Canada's

HOW INTERNAL AUDIT CAN HELP ADDRESS SEXUAL HARASSMENT RISKS

Internal audit has a responsibility to provide assurance that risks around sexual harassment policies, procedures, and reporting are being managed.

- » Follow U.S. Equal Employment Opportunity Commission guidance, Proposed Enforcement Guidance on Unlawful Harassment (January 2017), which sets the expectation that employers are being proactive in eliminating workplace harassment. It also outlines five core principles that have proven effective.
- » Make sure there is a written policy on how to handle harassment, discrimination, or retaliation claims. The absence of a written policy almost automatically triggers liability, Brian Koegle says. Policies need to address everybody in the liability universe—full-time and part-time employees, independent contractors, vendors, and clients who each pose some risk of potential liability.
- » Make sure company codes of conduct include examples of inappropriate behavior, Ed Lynch advises. Relevant examples are critical, he says, "because they serve as bright lines and consequently need to be continuously updated to reflect the changing work environments within each company."
- » Human resources should conduct training and communicate to employees about how and where to report sexual harassment. Even with policies in place, not everyone knows the process for reporting.
- » Make sure there is an anti-retaliation policy. Inform personnel that the hotline may not only be used for obtaining information and reporting concerns, but also for reporting issues of retaliation. The code of conduct should plainly state that retaliation against anyone reporting harassment in good faith is a significant, punishable violation.
- » Compliance isn't enough. Testing the effectiveness of compliance programs is another step and leveraging them to mitigate underlying risk is still another. That's part of the reason The Committee of Sponsoring Organizations of the Treadway Commission has an internal controls framework and an enterprise risk management framework.
- » Internal audit or the chief compliance officer should report on the effectiveness of a company's hotline to the audit committee. "Having lines of communication and, ultimately, an objective, confidential hotline process to lodge concerns to someone from outside that unit who will investigate is a critical control," Betty McPhilimy says. "You don't want hotline complaints squelched by a senior manager. They should go up to the board so people feel the hotline is a credible resource."
- » Don't reinvent the controls wheel. Risk management around harassment usually requires no new tools. An organization's performance reviews, open-door policies, escalation procedures, ombudsmen, incentives, disciplinary action procedures, and ethics and compliance hotlines are all designed to accommodate anything that comes up, including sexual harassment.

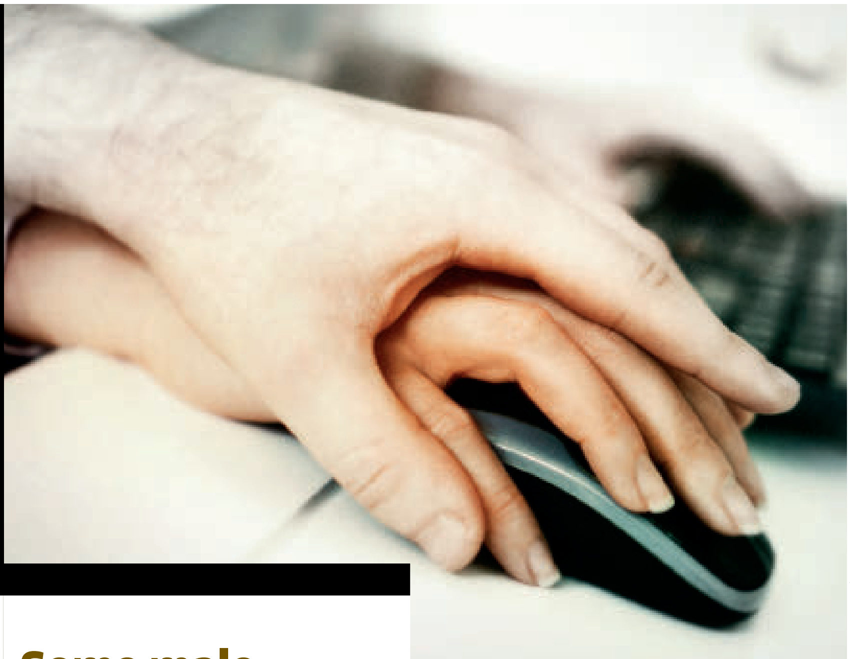
Heritage Minister told CBC News that arts organizations lacking best practices for harassment and bullying also may be blocked from future funding.

- After sexual harassment allegations targeted former CEO Steve Wynn, the *Boston Herald* reported that a casino under construction there would probably not carry Wynn's name. Wynn stepped down and sold his shares, but the allegations caused Wynn Resorts stocks to plummet. Wynn reportedly settled one harassment suit for $7.5 million; regulators in Nevada and Massachusetts and in Macau, China, are examining the company.

The secondary risk organizations face is civil litigation saying the company didn't do an appropriate job of providing a safe workplace, Kuling says. The government of Alberta recently amended safe workplace legislation to include mitigating the risk of discrimination and harassment, for example. "Harassment can be treated as a workplace injury," he explains, creating regulatory risk as organizations prepare for and comply with their obligations under the law.

The third risk that's developing, Kuling adds, "is where internal auditors can do a much better job: employee turnover." People who don't report harassment may just leave, he explains, and not mention the reason during exit interviews. But when internal audit conducts culture assessments, investigators "might get indicators of harassment and discrimination issues," he says, adding that "the professional skepticism of internal auditors has to come to the forefront. That data could then inform future audits of turnover statistics."

An ongoing culture of harassment and discrimination, Kuling argues, In light of recent headlines, 69% of surveyed CAEs have not provided more detailed risk information in regard to sexual harassment/misconduct to their boards, according to an AEC Quick Poll.



DMITRI MA / SHUTTERSTOCK.COM

Some male investors have declined one-on-one meetings with women ... BECAUSE THEY WORRY ABOUT COMMENTS BEING MISUNDERSTOOD.

even if localized to a department, "is going to be hard to hide." Lynch agrees and adds that internal audit should be prepared to identify and report suspicious behavior while working every assignment. "The nature of internal audit brings the auditor in contact with a wide range of employees," Lynch says. "Every internal auditor should receive training on identifying evidence of sexual harassment, or a failed reporting mechanism, and every audit report should provide an opportunity for the auditor to comment on compliance with the code of conduct."

BEING PROACTIVE

Organizations need to act, Kuling stresses. "Boards of directors need to have conversations with executive leaders around the culture of their organizations, and then be prepared to invest time and resources to seek assurance that these risks are being managed appropriately." Deynes adds: "Internal audit can assist human resources in designing processes that confidentially discover existing problems and report them to the appropriate internal or external authorities. Legal can and should provide all necessary avenues for the execution of severe internal penalties and external prosecution for offenders."

But organizations must ensure they don't attack harassment with processes that simply separate the sexes. *The New York Times* reported that "some male investors have declined one-on-one meetings with women or rescheduled them from restaurants to conference rooms" because they worry about comments being misunderstood and becoming career-enders.

"That's bad," says Phyllis Hartman of PGHR Consulting Inc. in Freedom, Pa. "Clearly, we have to work together, and we've got to help people communicate respectfully, even when perceptions differ as far as how and when to say 'lay off' and end it then and there." When managers say they're afraid to talk to female employees, she tells them: "You probably can't get into trouble talking about work. It's highly unlikely you'll be falsely accused." And if a woman finds herself in a situation where she is "systematically excluded from important meetings and opportunities" or if her supervisor acts "in ways that adversely affect her advancement opportunities, learning opportunities, and so on," she could legally claim discrimination under the Civil Rights Act of 1964.

HANDLING HARASSMENT

What happens after sexual harassment is reported is critical, and internal audit has an important role in ensuring retaliation isn't tolerated. Those acts, the NWLC points out, include a reprimand or other discipline, including termination; transfers to less-desirable positions or work schedules; and threats to report people to law enforcement based on immigration status. In some cases, just the threat of being penalized for speaking up constitutes retaliation, because the risk of career damage or being labeled a troublemaker is real.

Enforcement varies by jurisdiction. In Europe, member states are bound by the European Commission's Directive 2006/54/EC, which defines sexual harassment as conduct intended to "violate the dignity of a person by creating an intimidating, hostile, degrading, humiliating, or offensive environment," and Directive 2012/29/EU, which requires "assessments to determine if victims are at risk of retaliation"—and calls on employers to "offer appropriate


DON'T JUST FOLLOW RULES.
HAVE STANDARDS.

MORE **VISIT "Into the Light" on InternalAuditor.org for additional content about sexual harassment in the workplace.**

measures to protect them." In the U.S., claims of workplace harassment and retaliation are handled differently by state. California, for example, is particularly aggressive, maintaining "an affirmative legal obligation to protect victims from retaliation," Koegle says. "This includes requiring employee handbooks to address with specificity what you do to investigate, remediate, and prevent acts of retaliation."

A recent Harris Poll/CARE survey found that sexual harassment in the workplace isn't illegal in nearly one-third of the world. One-third of respondents in India said it's acceptable to whistle at colleagues, about the same as the portion of U.K. respondents from 25 to 35 who think touching a co-worker's buttocks is fine.

ADDRESSING THE FUTURE

Rehabilitation also is an important process concern, Hartman points out. In most cases, victims don't want accusers fired, they just want it to stop—but returning an accused executive to meaningful leadership "takes a lot of work," she says. "You have to help both parties deal with this, making sure perpetrators understand what they did wrong." For victims, counseling is a good place to start, according to research published in *Psychotherapy: Theory, Research, Practice, Training,* the journal of the American Psychological Association. But the specifics, says Kuling, are best left to each to determine. "The complainants are the best source of what constitutes adequate resolution," he says.

Counseling often helps the alleged perpetrators, too. Hartman has coached executives accused of inappropriate behavior whose companies felt they could be rehabbed, often as a condition of returning to their former posts, and she stresses that success is situational, depending on what happened, how the two parties work together, and what the workplace is like.

HARASSMENT DOESN'T DISCRIMINATE

Most types of workplaces have faced harassment challenges, including universities, hospitals, and government.

- Higher education has taken more than one hit in cases that go far beyond harassment. Michigan State University (MSU) faces recurring headlines related to assault complaints against disgraced former staff and Olympic gymnastics team physician Larry Nassar and other school officials. Johns Hopkins University paid almost $200 million to about 8,000 former patients of deceased gynecologist Nikita Levy to settle 2014 charges involving his use of a concealed camera to photograph them during exams. And at Pennsylvania State University, the conviction of former president Graham Spanier and a new movie about former head coach Joe Paterno have kept alive the sexual misconduct case against former assistant coach Jerry Sandusky.
- A 2016 Research Letter published in the *Journal of the American Medical Association*, "Sexual Harassment and Discrimination Experiences of Academic Medical Faculty," reports that 30 percent of women on medical faculties experience sexual harassment. Its author says, "harassment is more common in fields where there are strong power differentials."
- In 2017, women working for U.S. Congress were "making fresh allegations of sexual harassment against unnamed members," according to CNN. The Office of Compliance, which handles harassment complaints against members of Congress, paid victims more than $17 million, in 268 settlements, from 1997 to 2017—including claims for racial, religious, or disability-related discrimination.
- TheHill.com recently reported that "state legislatures across the country have reeled in recent months under allegations that legislators harassed or assaulted staff, lobbyists, and even colleagues." The website noted that more than a dozen have resigned, and some have been expelled.

STAYING FOCUSED

It may trace its roots to a little hashtag and just five letters, but the media movement behind workplace sexual harassment has "helped organizations pay attention and give it serious thought," McPhilimy says—and that implicates internal audit. "Part of internal audit's role is looking for risks in human resources and employment," she explains. "We have a big role to play in ensuring controls are in effect in hiring, managing, and evaluating personnel and ensuring effective interactions." Essentially, making sure that there are training programs and policies and procedures that are documented, current, and effective. That's a role internal audit always plays, of course. "It's just that in the past, internal audit wasn't so focused there," she adds. "Maybe senior management didn't think of internal audit as an effective tool for determining if there are problems in such areas. Particularly as it becomes a higher profile risk, though, that's something internal audit should address with senior management." Ia

RUSSELL A. JACKSON *is a freelance writer based in West Hollywood, Calif.*

Tailoring IPPF Implementation

Urton Anderson, Andrew Dahle, Alice Mariano

Maturity models can help internal audit departments of varying sizes scale their approach in applying the framework.

A fundamental challenge of today's chief audit executive (CAE) is matching internal audit to the needs of the organization and the expectations of internal audit's key stakeholders. While there is one International Professional Practices Framework (IPPF) and one *International Standards for the Professional Practice of Internal Auditing*, internal audit functions vary in their practices and level of development across organizations. A primary role of the CAE is to tailor the application of the IPPF to the organization, taking into account its unique needs and environment and knowing how to leverage a maturity model view of the IPPF and *Standards* in striving for internal audit excellence.

A LIVING FRAMEWORK

One of the strengths of the IPPF is the principles-based nature of the *Standards*. Being principles based allows organizations of different industries, sizes, and locations — with varying governance models and stakeholder expectations — to apply the same set of standards. The principles-based nature of the *Standards* also helps add clarity and consistency, while still being relevant and adaptable to evolutions in society and in the organizations internal audit serves.

In 2015, the IPPF received significant enhancements that improved its ability to serve as a tool for internal audit functions to take their practice to higher levels of effectiveness and provide even greater value to their organizations. Two noteworthy changes are:

- » Creation of the 10 Core Principles for the Professional Practice of Internal Auditing, which, taken as a whole, articulate internal audit effectiveness. For an internal audit function to be considered effective, all principles should be present and operating effectively. However, with the release of these Core Principles, The IIA also recognized that how an internal audit function demonstrates achievement of the Core Principles may differ from organization to organization.
- » Implementation Guides and Supplemental Guides moved from "strongly recommended" status to "recommended" status, adding further flexibility to the IPPF for practitioners.

The ever-evolving nature of the IPPF gives practitioners the flexibility they need to align to the unique needs of the organizations they serve. The IPPF's various layers also provide practitioners with a framework they can use to continually integrate new methodologies, tools, resources, and practices to further mature their performance.

A MATURITY MODEL VIEW

When looking at internal audit's conformance with the *Standards*, many practitioners and stakeholders at first may think of it as a binary exercise—either being in conformance or not. Perhaps this is natural given the external quality assurance and improvement assessment's common ratings scale of "generally conforms," "partially conforms," and "does not conform" are widely recognized.

Practitioners should look at using the IPPF and the *Standards* as part of a journey toward greater maturity and continuous improvement. Such a continuous improvement view is consistent with the IPPF, which includes in the *Standards* the assertion that quality is not only about assessing quality at one point, but also about improvement, as outlined in Standard 1300: Quality Assurance and Improvement Program. A maturity framework approach allows practitioners to assess the audit function's implementation of the IPPF to continually improve audit practice.

MATURITY MODEL STRUCTURE

Many organizations have used maturity models to assess and help bring continuous improvement. The IPPF, itself, includes guidance on the use of maturity models, including The IIA's Practice Guide, Selecting, Using, and Creating Maturity Models: A Tool for Assurance and Consulting Engagements. Based on review of other maturity models, the following categories are proposed for use in the model for applying the IPPF: Level 5 – Optimized, Level 4 – Managed, Level 3 – Defined, Level 2 – Repeatable, and Level 1 – Initial/Ad hoc.

It is natural to ask how these levels align with the category of general conformance to the *Standards*. For consistency, and to allow the maturity model to capture performance that falls below general conformance—as well as above the base general conformance level—Level 3 on the maturity framework will be defined with attributes that achieve general conformance with the *Standards* (see "Maturity Model Alignment Points" on page 31).

APPLYING THE MATURITY MODEL TO THE *STANDARDS*

By exploring several areas of the *Standards,* one can see how the maturity model may be applied. Some aspects of the *Standards* may seem binary, such as Standard 1000: Purpose, Authority, and Responsibility, which requires that an internal audit activity have a charter. Either an organization does or does not have an internal audit charter.

EXAMPLES OF SUCCESSFUL USES OF MATURITY MODELS

- » The IIA's Internal Audit Capability Model for the Public Sector
- » The Internal Audit Maturity Assessment – previously maintained by The IIA Quality Services Department
- » IIA Path to Quality Model
- » IIA Practice Guide, Process Capability Maturity Model
- » IIA Practice Guide, Compliance and Ethics Program Maturity Model
- » The ISACA COBIT 4.1 Model
- » The RIMS Risk Maturity Model
- » Software Engineering Institute Capability Maturity Models
- » International Organization for Standardization and the International Electrotechnical Commission's ISO/IEC 15504

TO COMMENT on this article, **EMAIL** the authors at urton.anderson@theiia.org

MATURITY MODEL ALIGNMENT POINTS

MATURITY LEVELS	STATE OF INTERNAL AUDIT	STANDARDS CONFORMANCE
5 - Optimized	Fully aligned with the organization, high stature and support, innovating, very highly valued, aspirational	Conforms with *Standards*
4 - Managed	Proactive, continuously improving, automatically monitored, insightful and impactful, sustained, highly valued	
3 - Defined	Professional, uniformly applied, mature quality program, embedded in documented practices and processes, valued	
2 - Repeatable	Established, has a standard pattern, minimum coverage, gaps with stakeholder expectations	Not in conformance with *Standards*, perhaps partial conformance
1 - Initial/Ad Hoc	Being developed, in early stages, not consistent or of high stature, reactive	Does not conform with *Standards*

However, even given this binary nature, the maturity model can be used to highlight how to differentiate between conformance in Level 3 – Defined and below conformance (Level 2 – Repeatable and Level 1 – Initial/Ad Hoc). Perhaps even more importantly, note how Level 4 – Managed and Level 5 – Optimized can be used to differentiate higher levels of maturity and excellence, using the charter as an opportunity for stakeholder engagement, alignment, and elevation of internal audit stature and opportunity to perform (see "Internal Audit Maturity Model Related to the *Standards*" on page 32).

A fundamental area such as communication of results applies to every internal audit function. The column, "Standard 2400: Communicating Results," in the "Internal Audit Maturity Model Related to the *Standards*" chart at the base levels cover aligning the report with core points in the *Standards*. The higher levels of 4 – Managed and 5 – Optimized include exploring stakeholder value and insights received, as well as stakeholder, top executive, and board perceptions on the quality of internal audit reporting.

Lastly, talent is an area of importance and challenge for many internal audit functions, so using a maturity model approach to look at Standard 1000: Proficiency and Due Care, or any other standard to apply the IPPF, can identify an array of practices and performance levels that can result in distinct improvements.

Currently, internal audit functions often look for leading practices, opportunities to provide more value, and continuous improvement. Taking a fresh view of the IPPF and the *Standards* through a maturity model approach can help internal audit assess its current state, identify opportunities for improvement aligned with stakeholder priorities, and drive continuous improvement. Having a maturity model can equip the CAE with a framework and tools to help articulate options to stakeholders and the internal audit team. CAEs need to

INTERNAL AUDIT MATURITY MODEL RELATED TO THE *STANDARDS*

	Standard 1000: Purpose, Authority, Responsibility
5 – Optimized	» The internal audit charter reflects a broad coverage of governance, risk management, and control. » The stature and trusted advisor status of internal audit is evident in the tailored definition of internal audit's responsibilities. In the right key management activities, internal audit is authorized to have a seat at the table. » The audit committee charter is aligned with internal audit's charter and vice versa. This may include the substance of the audit committee's activities, given the functional reporting line for internal audit. » The internal audit charter supports internal audit's role in the Three Lines of Defense.
4 – Managed	» The discussion on charter updates is used to challenge the organization on whether internal audit's coverage and stature is sufficient. The discussion also is used to challenge internal audit on whether it is aligned with the direction of the organization and is delivering on the commitments in the charter. Continuous improvement comes through the process. » The charter is reviewed and approved as part of a defined cadence, likely annually.
3 – Defined	» The charter is defined and periodically reviewed and approved. » The charter is generally aligned with the Model Internal Audit Activity Charter (http://bit.ly/2r1NI37).
2 – Repeatable	» Internal audit has a charter that was approved, but it: » Has not been updated. » Is generic. » Does not appear to align with the strategies, objectives, and risks of the organization. » Does not appropriately position internal audit. » Under-resources internal audit. » Does not promote an insightful, proactive, and future-focused internal audit activity.
1 – Initial/ Ad Hoc	» A charter does not exist, is outdated, or has not been approved outside of the CAE.

be adept at defining those aspects of applying the maturity model approach that will make a difference in their organization, given the stakeholder expectations and risks.

DOES SIZE IMPACT MATURITY?

Beyond maturity levels, internal audit, itself, varies in size as does the size of the organization it serves. A smaller internal audit function may not need as much documentation in planning and process as functions serving large, complex organizations. Some elements, such as an internal audit charter, will apply no matter what the size of the organization; however, other aspects of the IPPF, such as how to build talent models, may not require the complexity of infrastructure.

The IIA's Practice Guide, Assisting Small Internal Audit Activities in Implementing the *International Standards for the Professional Practice of Internal Auditing*, notes the level of challenge for a small internal audit function in conforming with various categories of the *Standards*:

- Low degree of challenge: Standard 1000: Purpose, Authority, and Responsibility.
- Medium degree of conformance challenge: Standard 1100: Independence and

Just 58% of CAEs say understanding the IPPF is essential to their audit function's ability to perform its responsibilities, according to the 2018 North American Pulse of Internal Audit.

Standard 2400: Communicating Results

- Internal audit leverages communication vehicles similar to other innovative areas in the organization, such as video summaries, periodic updates, and a website.
- Internal audit communications are seen by the audit committee and management as some of the most insightful communications on key risk areas, and they leverage the reports for other purposes in the organization.
- Internal audit issues an overall opinion on the state of risk management and control in the organization, and that opinion is supported by sufficient work.

- Internal audit reports are highly valued by the audit committee, the organization, key stakeholders, and process owners.
- Internal audit receives strong positive feedback from clients on its engagement communications.
- Internal audit communications are crisp, with effective executive summaries.
- Internal audit communications share lessons learned from reviews as well as leading practices with similar units in the organization.
- Internal audit issues opinions/ratings on engagements.

- Internal audit communicates effectively, including reports that are consistently accurate, objective, clear, concise, constructive, complete, and timely.
- Internal audit reports lead to organizational improvement.

- Internal audit reports are usually accurate, objective, clear, concise, constructive, complete, and timely.

- Internal audit reports are issued, but not always timely, and at times they create unnecessary challenges in the process due to accuracy or professionalism.

Objectivity, Standard 1300: Quality Assurance and Improvement Program, Standard 2000: Managing the Internal Audit Activity, Standard 2200: Engagement Planning, and Standard 2300: Performing the Engagement.

- High degree of conformance challenge: Standard 1200: Proficiency and Due Professional Care, Standard 2100: Nature of Work, Standard 2400: Communicating Results, Standard 2500: Monitoring Progress, and Standard 2600: Communicating the Acceptance of Risks.

For an audit department covering a smaller, less complicated organization, some of the higher levels of internal audit maturity may not be needed. However, some aspects of internal audit excellence that are money and time saving may be as important in a smaller, closely aligned, agile organization as in a large, international conglomerate.

In a small internal audit department, the challenges can be addressed through flexible planning, process disciplines that keep everyone on track, and tools available to CAEs of small groups. For example, flexibility can be applied during internal audit risk assessments, in duration and style of internal audit projects, and in documentation and communications. In process discipline, internal auditors should focus on what is important to accomplish and eliminate the unnecessary, strive to automate repetitive tasks, and leverage checklists and lessons learned to continually improve.

Many tools and resources are available to internal audit groups of all sizes and maturity levels, thanks to The IIA, the internet, and peer networks. There also are many technology solutions that can help ease the administrative needs of small departments by facilitating standard workflows, approval/review processes, and action plan follow-up. Having a robust system can be a key source for demonstrating compliance with several of the standards. Ia

URTON ANDERSON, PHD, CIA, CRMA, CCEP, *is an EY Professor and Director of the Von Allme School of Accountancy at The University of Kentucky in Lexington.*
ANDREW DAHLE, CIA, CPA, CFE, CISA, *is a partner in PricewaterhouseCoopers' Risk Advisory Services in Chicago.*
ALICE MARIANO, CIA, CPA, CPCU, *is director of internal audit for North Carolina Farm Bureau Mutual Insurance Co. in Raleigh.*
Anderson and Dahle are co-authors of Applying the International Professional Practices Framework, 4th Ed., *published by the Internal Audit Foundation.*

Find *your*

VOICE

KAREN BRADY, 2018–2019 chairman of The IIA's North American Board, wants internal auditors to communicate their value to ensure their ongoing relevance in a rapidly changing world.

Photographs by Betsy Hansen

The nature and role of internal auditing in North America has radically altered over the past decade or so. No longer seen as a back-office compliance department, there just to check accounts payable or perform mundane administrative processes, the cutting-edge audit function is increasingly regarded by audit committees and regulators as a trusted advisor. Many chief audit executives (CAEs) have a seat at the top table, advising the C-suite on emerging and strategic risks and helping management mitigate those threats to the organization's objectives.

Internal audit has had to work to implement those changes to its role and status, and I have great respect for the courage and determination that takes. But not all internal audit functions are operating at that level. That could be because stakeholders do not fully understand what internal audit does—or can do—and continue to underinvest and undervalue their audit functions. Or, it may be because internal auditors do not always push as hard as they might to fulfill what can be a daunting and uncomfortable role.

My theme as chairman of The IIA's North American Board over the coming year is "Find Your Voice." Specifically, I want all internal auditors to reflect on, develop, extend, and communicate the true value they can provide to their organizations. In finding their voices, auditors will be able to achieve their full potential in serving their organizations, and they will be ensuring their ongoing relevance in a rapidly changing world.

EXTERNAL PRESSURES

There are two major trends that make my message urgent. For the first time in many years, there is an emphasis in the U.S. government on deregulation. This is a radical change from the increasing levels of rulemaking and regulatory scrutiny the profession has faced since the turn of the century.

Both the U.S. Sarbanes-Oxley Act of 2002 and the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act, as well as countless other pieces of regulatory reform, have tended to emphasize the compliance function of internal audit. If stakeholders, especially in the energy and financial sectors, for instance, see internal audit as a box-ticking function, it is largely as a result of these requirements.

Since Donald Trump became president, an estimated 600 regulations have been eliminated, according to George Washington University's Regulatory Studies Center. High-profile examples include the partial repeal of the Dodd-Frank Act, the repeal of the Affordable Care Act individual mandate, and the Federal Communications Commission privacy rules.

If internal audit's key stakeholders, including audit committees, believe that most of internal audit's value comes from ensuring the organization complies with regulations, it does not bode well. They may believe that if the regulations disappear, internal audit will not be needed. This could not be further from the truth. Indeed, while regulations may be eliminated, the risks addressed by them will continue to exist. If anything, risks and the related need for internal audit services increase in a deregulated market. Still, it appears conditions are not prime for internal auditing to become a mandated function within organizations in the foreseeable future.

A recent IIA global study on the regulation and licensing of internal audit reveals a consensus among stakeholders that, for several reasons, governments should not regulate or mandate internal audit. Regulation can take away decision-making from management and the board, say respondents to the study.

Regardless, this has not stopped The IIA from moving ahead with a strategy to advocate for a comply-or-explain mandate for publicly traded companies. Under such a mandate, organizations would have to report whether they have an internal audit function and how it is resourced. If they do not have an internal audit function, they would have to explain how they are mitigating risks. Such disclosure provides an increasingly active investor community vital information about a company's approach to risk management. But in the interim, internal audit should become an integral part of an organization as the result of a carrot, not a stick.

The second major trend revolves around advances in artificial intelligence (AI), robotic process automation, and other technologies that threaten to replace compliance-based auditing. Internal auditors should fully grasp the implication of such automated auditing. Thomas Sanglier's recent book, *Auditing and Disruptive Technologies*, published by The IIA's Internal Audit Foundation, rightly argues that to thrive in the near future, audit departments will need to adopt and adapt to such advances. Staying relevant to organizations will mean moving up the value chain so that audit is operating at a strategic level. Technology will process the data.

This is why internal auditors need to tell their stakeholders how valuable effective, strategic, risk-based auditing can be. We can help them see the bigger risk picture by getting involved in supporting the strategic objectives of our organizations. Granted, AI will replace some of the traditional roles and tasks that internal audit has performed, but, in my view, it would be a welcome relief to move away from the humdrum compliance work and start focusing exclusively on what really matters—start focusing, in short, on value.

DEFINING VALUE

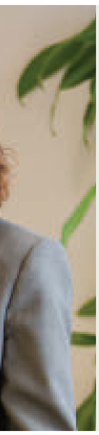
There are many definitions of *value*, because the concept changes over time as the demands on internal audit evolve. The IIA's International Professional Practices Framework is

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

a good place to start. It says, "the internal audit activity adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management, and control processes; and objectively provides relevant assurance."

Putting those sound principles into practice can be more difficult than it might first seem. For example, what is relevant assurance? How can internal audit become more involved in strategic objectives and risks if that is not what stakeholders seem to be expecting? And how do stakeholders understand the value that internal audit can offer?

> **There is a real risk that stakeholder expectations are based on outdated notions of internal audit.**



There is some truth to the idea that internal audit's value resides in the eye of the beholder—the board, management, regulators, and other external parties. But we cannot be a passive recipient of those views if they do not mesh with contemporary practice. There is a real risk that stakeholder expectations are based on outdated notions of internal audit.

For example, one of my stakeholders is an incredibly knowledgeable individual—a former Big Four partner who is heavily involved in his own professional bodies. Recently, I told him we were doing the annual risk assessment and he surprised me by asking why internal audit was doing so. I explained how performing our own risk assessment helps internal audit create a risk-based audit plan and helps the organization achieve its strategic goals. I was glad that he had come to me because, frankly, I assumed he knew what internal audit did.

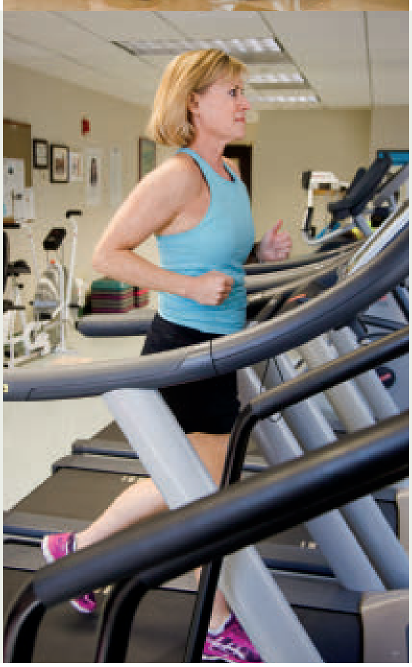
The first step to defining your voice is to create a value statement. Examples might include, "external auditors audit the past, we audit the future." Or, "internal audit assists the board and management in accomplishing their responsibilities." Or simply, "internal audit helps make the organization more successful." Be sure to consult internal audit's stakeholders. Creating a value statement is most effective when the process engages all involved. It is an opportunity to build understanding within the audit team about how audit is perceived and to explain to stakeholders the value internal audit could be offering where that is poorly understood.

Any value statement has to be addressed to the audience it is intended to inform—so while I urge auditors to advocate and educate stakeholders, they must do so in a language that is free from jargon. Because I work for a not-for-profit organization, my audit committee is made up of members of our community. That includes some financial experts, but also a Baptist minister, a real estate agent, and a couple of other individuals who do not have finance and business backgrounds. While they are smart people, I need to be able to explain internal audit's value in a way that makes it easy for me to demonstrate what we have achieved through our work for the business. Creating a clear and well-understood definition of internal audit's value for all stakeholders is a powerful tool.

WALKING THE TALK

In addition to advocating for an enhanced role and communicating with, and listening to, stakeholders, internal auditors need to deliver on their promises. Each of us needs to be the best internal auditor he or she can be. That involves being well-educated about the technical aspects of internal auditing, being up-to-date on current and emerging trends, and making a solid commitment to improve and update those soft skills that are crucial to our roles. Internal auditors should be certified to demonstrate their professionalism. Also, I am a big advocate of volunteering in the profession, of joining local chapters or committees and getting involved. I have benefited greatly on both counts. I am up-to-date on best practices and emerging issues in internal audit, and my organization has benefited from the technical skills I have obtained through my participation. At the same time, I have met some amazing people and developed some great friendships.

One area that CAEs often overlook is using external quality assessments as a challenge to the board. All internal audit departments should undertake periodic quality assessments, as mandated by The IIA's Standard 1312, which says an external quality assessment must be performed every five years. I accept that it can be a difficult process to go through, but it can also be a tool for change. Presenting the results of such a review to stakeholders can support the CAE's constant requests that the function be involved in more strategic and challenging work. If CAEs know they are not using audit staff most effectively, the quality review will reflect that in an evidence-based way. It is another way



ADVOCACY TOOLS

Internal auditors should make full use of The IIA's advocacy tools to inform their stakeholders of the value an effective function can provide. These include the Global Advocacy Platform: Pillars of Good Governance (http://bit.ly/2Hyvw2C) and the position papers (http://bit.ly/2HzeXnn):

- The Three Lines of Defense in Effective Risk Management and Control
- The Role of Internal Auditing in Enterprise Risk Management and Control
- The Role of Internal Auditing in Resourcing the Internal Audit Activity
- Internal Audit's Role in Good Governance (available later in 2018)

In addition, auditors can take advantage of relevant *Internal Auditor* magazine articles (InternalAuditor.org) to get up to date in best practices and share those with their stakeholders, where appropriate. Some recent examples include:

- "5 Steps to Marketing Your Audit Department"
- "Your Personal Brand"
- "Board Matters"
- "The Dynamics of Interpersonal Behavior"

THE 2018-19 NORTH AMERICAN BOARD CHAIRMAN

Karen Brady began her career with Ernst & Young in New Orleans and has served in various executive positions, including controller and chief audit executive within the hospitality industry. She is a Certified Internal Auditor and Certified Fraud Examiner and has her Certification in Risk Management Assurance.

Today, Brady is the corporate vice president of audit and chief compliance officer for Baptist Health South Florida. Baptist Health is the largest, CAEs can find their voice and demonstrate that the audit committee can get real value from its audit function.

Being the best can be challenging and sometimes lonely. It can take time, effort, and patience to get the message through that internal audit is a forward-looking and progressive part of the business when those around you do not necessarily share or understand that view.

It can take time and patience to get the message through that internal audit is a forward-looking part of the business.

To stand in front of a stakeholder and say, "I'm supposed to be involved in strategic initiatives and have a seat at the table" is not always successful or well-received. To further support auditors, The IIA's North American Board is putting more emphasis on advocating for members—an approach I will continue and extend where possible. It is no longer enough for The IIA's advocacy to focus on attending meetings in Washington, D.C., to try to influence legislation and advocate for better governance. Although this is incredibly important and we continue to push initiatives with the U.S. Securities and Exchange Commission and other regulators, The IIA also is appealing directly to stakeholders. For example, we are hoping to partner with organizations like the National Association of Corporate Directors (NACD) to make sure they have the tools to inform their members about what they should be looking for from their internal auditors. Many audit committee and board members belong to the NACD and similar bodies. There are many other organizations that serve CEOs, chief financial officers, and other groups, and The IIA North American Board will be advocating and educating on the value internal audit can provide to their members. I urge internal auditors to also advocate for themselves—to "find your voice." The IIA has many tools to assist you in this endeavor. For example, send copies of IIA advocacy documents to your stakeholders (see "Advocacy Tools," page 38). Sometimes it is more objective and compelling when it comes from a third party.

FINDING INTERNAL AUDIT'S VOICE

Obviously, what I have set out as my theme will take more than a year to achieve. But working together as a profession, and with our key stakeholders, we can help internal audit find its voice—and its place—to foster success and create opportunities in our organizations and beyond. Ia

KAREN BRADY, CIA, CRMA, CFE, *is corporate vice president and chief compliance officer, Baptist Health South Florida in Coral Gables.*

not-for-profit health-care organization in South Florida, including 10 hospitals and over 50 outpatient facilities spanning four counties. With more than 18,000 employees and over 3,000 physicians, Baptist Health is considered one of the nation's top employers, according to *Fortune's* 100 Best Companies to Work For. It also has been recognized by the Ethisphere Institute as one of the World's Most Ethical Companies for the past eight years. Brady has been with Baptist Health for over 25 years and during that time has implemented a robust, award-winning Internal Audit and Compliance department.

In addition to serving as North American Board chair and as a Global Board member, she has volunteered at The IIA in various capacities for many years. For example, she is a past conference chair (2011), Learning Solutions Committee chair (2011–2013), and Global Professional Development chair (2015–2017).

Brady also is past president of the Florida Health Care Compliance Association. Recognizing the importance of giving back to the community, she serves as chair of the Finance and Audit Committee on the Board of Riverside House, a charitable organization that helps guide men and women convicted of crime toward becoming productive citizens through a nondenominational, faith-based approach.

She is a fitness enthusiast and enjoys her morning runs. In her spare time, she enjoys travel, hiking, and water sports with her husband Jim.

Leading toward improvement

Wade Cassels, Kevin Alvero, and Randy Pierson

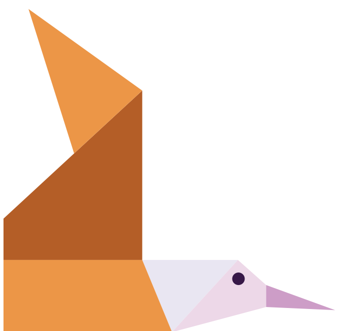
Audit managers can point the way to enhanced, cost-effective professional development for the audit function.

Ongoing professional development is not an extracurricular activity; it is integral to ensuring auditor competency and a requirement for auditing in accordance with The IIA's Code of Ethics. Beyond that, professional development plays an increasingly important role in recruiting and retaining talent that can meet the future needs of the audit function.

According to The IIA's 2018 North American Pulse of Internal Audit report, "CAEs will not be able to hire their way out of [the] skills shortage. … CAEs that develop talent continuously and consistently can identify gaps, strengths, and weaknesses in the internal audit activity." The report adds that internal audit functions that make provisions for career development programs will not only help themselves in terms of skills inventory, they will have an advantage in talent recruitment, development, and retention as well.

While each auditor must take responsibility for his or her own professional development, audit managers can play a key

MANGSAAB / ISTOCK.COM



role in ensuring the department receives the most value from these efforts and gives staff members the best chance for success. They can accomplish this by planning a coordinated approach to staff professional development, managing the development budget effectively, and cultivating a supportive culture that challenges individuals and rewards them for their efforts.

A COORDINATED EFFORT

According to the 2018 Pulse report, "Professional development plans with specific annual targets and provisions for training help to ensure a high level of collective proficiency for the internal audit activity." Although resources are available to help with planning, such as The IIA's Global Internal Audit Competency Framework, each audit manager must document skills versus needs specific to his or her own organization.

Planning for certifications and training can follow a two-pronged approach: On one side, audit managers should assess the skills and knowledge the department needs to fulfill its mission; on the other, they should consider the training and development progression of individual employees. This exercise should reveal clues as to where to focus staff training efforts, helping answer questions such as:

A brief, periodic email survey can keep managers up to date on team training.

- Where are there gaps? ("We need someone with the Certification in Risk Management Assurance and we don't have one; who would be the best person to pursue that?")
- How should the talent pipeline be organized? ("We are going to need another Certified Internal Auditor on staff within the next year; should we train or hire?")
- Where is there overlap? ("We have three people all working on the Certification in Control Self-Assessment; let's spread out.")
- Where do resources need to be deployed? ("We have a senior person with a lot of certifications; let's have her focus on publishing and presenting so we can devote study, application, and exam resources to lower level employees.")

To manage development efforts effectively, audit managers need to determine what kind of training employees want and then balance that input against the department's skill-related needs and budget. A brief, periodic email survey can be an effective tool for staying up to date on the teamwide training picture. For example, audit managers could ask:

- What are you working on now?
- In the past three months, have you earned a certification, published something, given a presentation, taken on a board/committee/volunteer role, or done something else that we need to recognize and celebrate?
- Do you know what the next step is in your training/development plan?
- Are there any impediments—such as lack of funds, time, or training materials—hindering progress on your training/development plan?

Job interviews, the onboarding process, performance reviews, and informal meetings also represent excellent opportunities to gauge what is important to employees, what they want to accomplish in their careers, and what types of training might help them meet those goals. Employees are more likely to remain committed to earning a certification if they believe they are helping

Only half of U.S. employees say their employer provides career development opportunities that meet their needs, according to a 2017 American Psychological Association survey.

both the team and themselves—that they are working toward bettering their future, rather than simply completing an assignment.

MANAGE COSTS AND STRETCH RESOURCES

Training and development can get expensive, but the audit department can make the best use of its professional development budget by taking advantage of cost-saving opportunities and by broadening its scope of learning activities. *Professional development* is sometimes used as a blanket term for passing certifications and maintaining them by earning continuing professional education (CPE) credits. Attending live seminars and purchasing online self-study courses are two of the most common ways auditors earn those CPEs. In addition to these methods, auditors can avail themselves of several other professional development resources.

First and foremost, auditors can take advantage of any free training and CPEs that align with their plan. For example, some professional organizations offer free webinars, and those free CPEs can add up to concrete savings by the end of the year.

Staff members also could volunteer to serve on an IIA committee, write for an industry publication, or conduct training courses and seminars. These are not only inexpensive ways to meet CPE requirements, they also serve as an effective means to promote continuing education and professional development above and beyond certification.

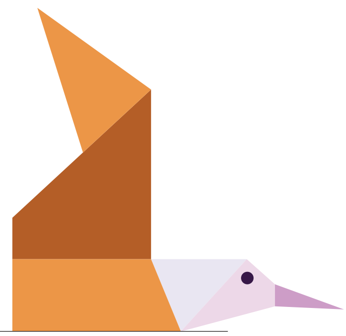
In addition to these approaches, audit managers can draw from a host of alternative resources and techniques. Each can be leveraged for training efficiency and cost savings.

CPE ACTIVITIES

According to Section 3.2 of The IIA's CPE policy, in addition to formal educational programs, certified individuals may obtain CPE through a variety of qualifying activities, including:

- Passing examinations.
- Authoring or contributing to publications.
- Translating publications.
- Delivering oral presentations.
- Participating as a subject matter expert volunteer.
- Performing external quality assessments.
- Taking *Internal Auditor* magazine's CPE Quiz.

Interdepartmental Learning Audit managers should consider sources for training from within their own company. Subject matter experts from other departments inside the organization can provide training on new technologies, business processes, etc., enabling audit staff members to better understand the business areas they audit. While internal training may or may not qualify for CPE, enhanced knowledge of the business will help improve auditors' confidence and enable them to offer more meaningful recommendations—making this highly valuable, and economical, training.

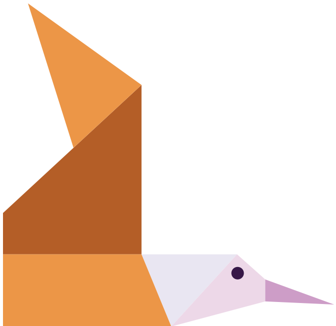


Audit managers can draw from a host of alternative resources and techniques.

Intradepartmental Learning
Managers can harness their own staff resources for budget-friendly training. For example, a staff auditor could be assigned to read a book from the Internal Audit Foundation

TO COMMENT on this article, EMAIL the authors at wade.cassels@theiia.org

and give a presentation to the team summarizing the book's content and its implications for the work internal audit does. This exercise not only adds new knowledge to the group, it also provides valuable public speaking experience and leadership training for the staff member—all at the mere cost of a book. Audit staff can also be a valuable source of experiential training. This is something the audit manager should consider as part of the overall professional development plan because certifications typically require some form of prerequisite experience. Job shadowing and working with more experienced auditors on a variety of engagement types can help auditors gain the experience they need to qualify for certifications.



Successful managers support training needs with work hours and funding.

Handing Down Knowledge Teamwork and collaboration also can help the audit department stretch its professional development budget. Mentoring, for example, can make the certification process more efficient. Auditors who have earned a particular certification can coach others seeking that certification, offering tips for taking the exam as well as advice on how to plan study time, how to navigate the application process, and which study materials are the most valuable (and least valuable). Passing down lessons learned like these can add up to large time savings, as opposed to having each new candidate begin the certification process from scratch.

Discounts and Group Savings Some organizations offer discounts on certification applications and exams at certain times of the year. The audit manager should incorporate these into the training plan so that auditors are working toward taking exams when they are the most affordable.

Auditors also can coordinate and save with group training opportunities, rather than having each staff member individually pursue certification and CPE. The IIA, for example, offers opportunities to obtain group savings on training courses. For events held by a local chapter, audit managers should always ask if a discount is available for group sign-up. Plus, some local chapters have funds available to provide assistance to members with costs such as conference travel and expenses as well as application and exam fees.

Training Library Finally, audit managers should consider creating a training library. The library can take on various forms (paper, digital, or both), and it should be available to any staff member seeking certification or training. This is the best way to economize the purchase of materials. Team members should not each buy the same training manual when they can plan ahead to stagger their study efforts and share purchased content.

A SUPPORTIVE CULTURE

Even though professional development is vital to an effective audit function, auditors can easily get caught up in their day-to-day work and relegate development to the cracks in their busy schedules. Audit managers can take several steps to help staff members resist this inclination.

First, managers should devote actual work time and resources to professional development. As the 2018 Pulse report states, a supportive culture for professional development is critical. Successful audit leaders not only preach professional development and certification, they back it up with the support of work hours and funding.

Employers identify **soft skills** as the No. 1 priority for talent **development,** followed by preventing skill gaps and understanding technology, according to LinkedIn's 2018 Workplace Learning Report.

Designating a professional development champion, in addition to the CAE, also can be helpful. The champion can assist the CAE with highlighting training opportunities, making sure team members who earn certifications are recognized, and connecting those seeking certifications with mentors who have already earned them. He or she also should be well-connected in the industry and thereby attuned to development opportunities, such as a chance for a junior auditor to volunteer on a committee, get a first speaking experience, or publish a first article.

Finally, the CAE and champion should work together to come up with ways to publicly recognize staff members for their professional development accomplishments. For example, whenever someone earns a certification, the champion could display the certificate in the office, ensure that it is mentioned in the department newsletter, and update the employee's business cards with his or her new designation. Whatever the method, accomplishments should be highlighted in some visible, lasting way. Recognition can be a powerful motivator, as it demonstrates to the individual that the department (and the audit leader) values and appreciates his or her effort. Moreover, it conveys to clients that audit personnel place a strong value and emphasis on professional development, and they possess the skills to not only do their jobs but to serve as leaders in their profession.

TOOLS FOR SUCCESS

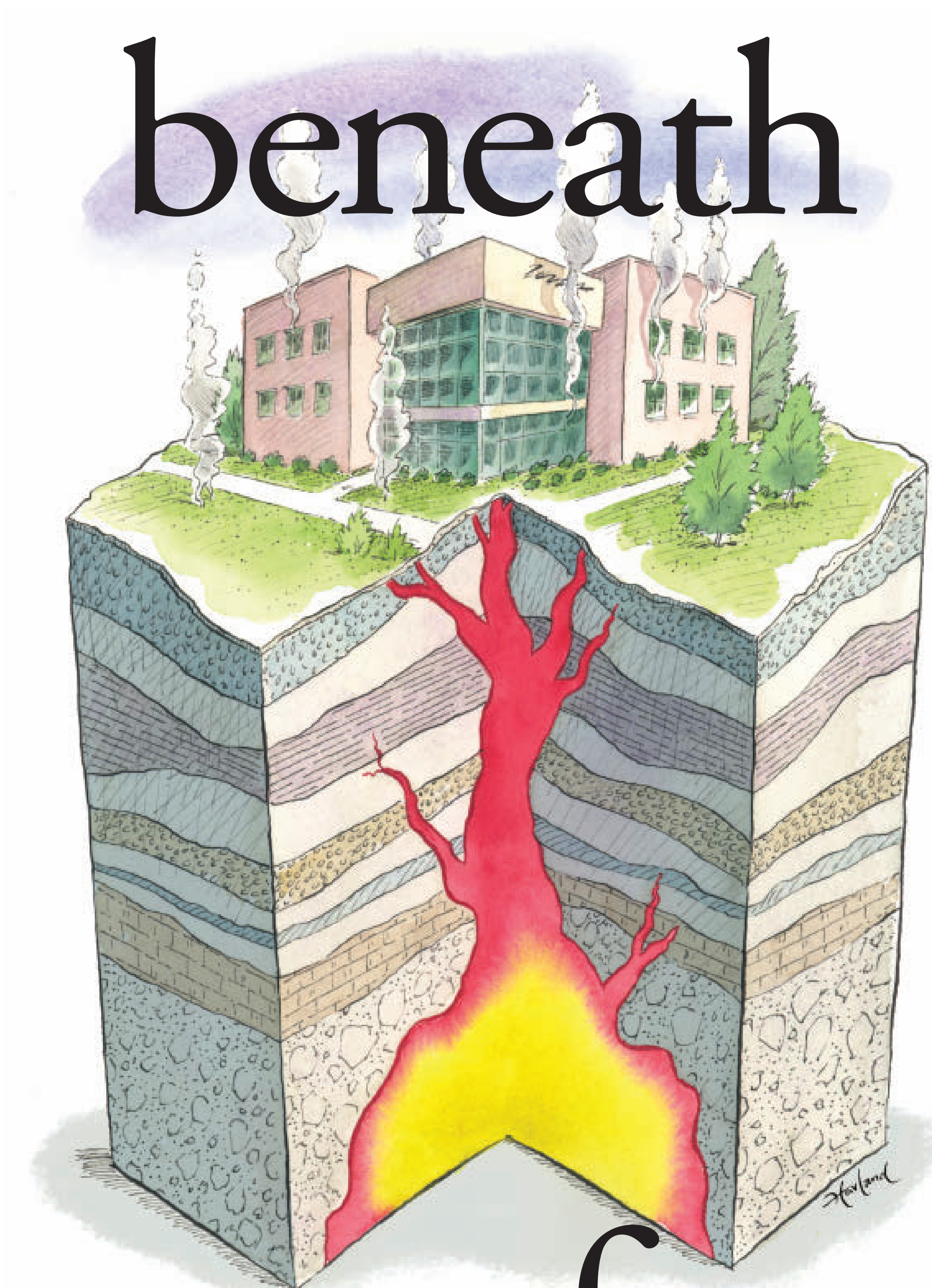
Ultimately, successful management of professional development resembles successful management of any other business process. The audit leader must align the mission and values of individuals with those of the organization, plan wisely, give people the tools and resources they need, and keep them engaged and motivated by tracking their progress and celebrating their success. The reward for the audit manager who does this effectively will be a greater ability to recruit and retain talent and to grow that talent to suit the mission of the audit function. Ia

WADE CASSELS, CIA, CISA, CFE, *is a senior auditor at Nielsen in Oldsmar, Fla.*

KEVIN ALVERO, CFE, *is senior vice president, Internal Audit, Compliance, and Governance, at Nielsen.*

RANDY PIERSON, CISA, CISM, CBCA, *is a senior auditor at Nielsen.*

beneath



the surface

Auditing culture requires practitioners to delve deep into the organization's core, beyond mere surface-level analysis.

Douglas J. Anderson

After wake-up calls from a long list of organizations—including Volkswagen, FIFA, and Wells Fargo—some observers might expect significant progress by now in addressing culture-related issues. But instead, high-profile cultural failures continue to plague the corporate landscape as the list of examples keeps growing.

Internal audit has a critical role to play in identifying and assessing problems with an organization's culture. Through a barrage of webcasts, presentations, and publications, most internal auditors are likely now attuned to the importance of examining this aspect of the organization. By now, practitioners should be aware that:

- Culture is a critical component of organizational governance and often the root cause of significant issues.
- Culture is not defined by documents and processes, but by employee perceptions and how things actually get done in an organization.
- There is no single culture in an organization, but a complex weaving together of multiple layers involving a tangled undergrowth of subcultures.
- There is no single right culture—optimal culture varies depending on the organization.

Still, many internal auditors have difficulty getting started with cultural audits, finding the subject matter hard to manage. Practitioners need to dig deep into this topic, well beyond the superficial mantle, and understand what to examine—as well as approaches to avoid. Stakeholders must have an accurate assessment of culture before damaging issues erupt in a torrent of organizational harm.

WEAK AUDIT EVIDENCE

Auditors like hard evidence, such as written approvals, formal contracts, and documented transactions. Hard evidence is objective, and typically it can be gathered by less experienced auditors and interpreted quickly.

Illustrations by Gary Hovland

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

In terms of auditing culture, hard evidence often relates to items such as:

- Communications from the C-suite on ethics — whether communications cover the important aspects of behavior and ethics and are sufficiently frequent.
- Ethics policies — whether policies are formalized, supported by training, and understood by the employees.
- Hotline calls — the number of calls, the policies on how calls are addressed, and evaluation of whether calls are addressed correctly.
- Turnover statistics — average sick time, rate of employee turnover, etc.
- Compensation programs — whether the programs are designed to reward the right behaviors and avoid incentivizing undesired behaviors.

These areas, and the hard evidence that can be obtained about them, certainly support culture. But even when programs and policies are in place and operating effectively, culture can still be a problem. Focusing on these aspects of culture is at best incomplete, and it could be misleading.

Culture is not primarily a set of policies and programs — it is defined through how employees behave in their day-to-day work. Expertly auditing and obtaining hard evidence has value, but it does not enable auditors to peel back the exterior of an organization and see what is really happening inside. Even surveys, though useful, provide limited insight on organizational culture (see "What About Surveys?" on page 49). Hard evidence cannot stand on its own and needs to be supplemented.

When considering evidence about culture, auditors may want to envision a volcano—where, from deep inside, lava and gases could erupt without warning.

STRONGER AUDIT EVIDENCE

When considering audit evidence about culture, internal auditors may want to envision a volcano — where, buried deep inside, lava and gases are collecting and could erupt from the earth's crust without warning. A volcano serves as an apt metaphor for how culture operates in an organization. On the outside, even when an eruption is imminent, everything might look fine. The form appears normal, the exterior is solid, and while a few small vents may show smoke, no major issues are evident.

Likewise, based on a surface-level assessment, the board and top management may conclude the organization appears sound. However, the effects of a toxic culture can be bubbling deep inside, and eventually an eruption occurs that no one seems to

Internal audit leaders say less than **5%** of their **audit plan** will be allocated to governance and culture risk over the next 12 months, according to The IIA's 2018 North American Pulse of Internal Audit.

WHAT ABOUT SURVEYS?

Client surveys might be convenient and produce hard data, but are they useful in auditing culture? Consider these observations:

» Culture-related issues that are significant enough to cause serious damage to an organization do not need to be widespread. A serious cultural issue that results in bribery in a foreign country, sexual harassment, or altering the accounting numbers in a noticeable way can occur in an isolated group of the organization because of a subculture unique to that group. Knowing that 99 percent of employees have not seen an incident of bad behavior is not helpful in detecting this type of issue.

» "Do senior executives keep their word?" is a question that may often be found in employee surveys related to culture. While this seems like a useful question, is it asking about all executives or excluding the one rogue executive? Does it encompass any kind of issue or only important ones? Does it apply to the last quarter or the last 10 years? An employee taking the survey likely does not have enough context to know how to answer, and the responses yielded will probably provide little useful information to the organization. Most survey questions seem to ask for responses in normal circumstances, for most employees, on average. This information will not identify a specific problem in a culture.

» Suppose employees observe an aspect of culture that is toxic. They may feel powerless to address it without jeopardizing their job. They may believe that if managers were truly concerned with culture, they would not have allowed this situation to persist. Upon receiving an employee survey from human resources, will they be motivated to answer the survey honestly? Aren't those caught in a toxic culture the ones who might hesitate to answer honestly, fearing their responses may not be anonymous?

Surveys can be useful, but they shouldn't be a primary source of evidence on culture. Although surveys can highlight certain issues and messages, they don't necessarily identify all important cultural issues. In this sense, surveys can provide a false sense of accomplishment and potentially neglect to identify hidden issues in culture.

have predicted. A problem remained buried in the mountain that could have been identified or predicted, yet no one uncovered the truth and brought it to light.

How can internal auditors help prevent, or at least caution about, the next eruption? Perhaps more importantly than looking at the organization's structures and foundation — the top-down, hard evidence — they need to get inside to see whether an eruption may be close at hand. A volcano contains a great deal of soft evidence, though examining these areas can be uncomfortable and somewhat risky. Diving deep into the organization to examine culture is the only effective way to perform the role required of internal auditing.

Where and when do auditors gather this soft evidence? Everywhere and all the time. Internal auditors do this primarily in two ways: as part of every engagement, and during their informal interactions with clients.

During Every Audit Internal audit projects provide an opportunity to get out of the office and engage directly with employees at all levels of an organization. Internal auditors should use this opportunity. Although focus groups and structured interviews can be somewhat helpful, they are artificial devices — participating in a prearranged session with an agenda, facilitators, note takers, and overseers is not the same as going about daily activities. Evidence pertaining to culture will more likely be identified after building relationships with audit clients and observing how they operate. On this foundation, culture will reveal itself to practitioners as they ask themselves several questions:

- How does management engage with the internal auditors? Throughout planning, fieldwork, and reporting, is management supportive of the audit or does it exhibit reactions ranging from dismissiveness, to a lack of

39% of **board members** say they receive information on **culture** from internal audit — the National Association of Corporate Directors' latest Public Company Governance Survey.

responsiveness, to outright interference with the engagement?

- Does management's style and approach foster the right mindset among employees in the group being audited? Does management reward the right behaviors? Does it communicate effectively and demonstrate transparency? Is it open-minded and accepting of new ideas? Do its actions reinforce that the end does not always justify the means?
- What is the tone of the employees in the area audited? Are they positive, supportive of management, and focused on the best interests of the organization? Do cliques exist within the group that hinder its success? Has groupthink so overtaken them that important ideas or concerns cannot be expressed?
- Are the core values of the organization expressed in what internal audit has observed? Most organizations adopt values around respecting people, doing the right thing, working collaboratively, or similar objectives. Do employees and management exhibit these core values throughout their activities, or are they all too willing to ignore them as they pursue alternative motives?

Beyond these topics, potential issues identified during an audit project need to be closely analyzed for their root cause. In fact, finding root causes related to culture is common. Given how frequently significant issues arise from toxic cultures, every audit issue should be examined to determine whether culture is part of the root cause.

One option to more formally bring culture into focus on audits would be to require the internal audit team to assess culture on each project. Initially the team may find this effort difficult, as evaluating all aspects of culture effectively takes experience and insight. The process is best learned through practice. Requiring a cultural assessment on each audit forces the practice, enables full consideration of different team members' perspectives, and helps build higher level observations on culture. If the team members on an audit project have insufficient experience auditing culture, their assessment does not need to be shared with client management. Audit managers can conduct the process strictly as an internal exercise until the team has gained the requisite level of competency.

Auditors need to stop the frantic pace of simply completing audit projects and consider what they observe in the different cultures in the organization.

While Walking the Hallways One of the major advantages of an internal auditor versus an external party is the ability to gain insight about the organization every day, from multiple angles. Internal auditors converse with all levels of employees as part of formal meetings, email exchanges, and even impromptu discussions in the hallways. They should use these interactions to gather evidence on culture, such as what is valued, what is rewarded, who is favored, and how problems are viewed. Moreover, effective internal auditors establish themselves as objective, unbiased professionals. In this capacity, employees will seek out the internal auditor to discuss their concerns and observations, providing further opportunity for cultural insight.

PULLING IT ALL TOGETHER

Whether through audit projects or walking the hallways, internal auditors should stay continually attuned to key audit evidence that may provide information on the organization's culture. Throughout the process, practitioners need to remember that a volcanic eruption caused by toxic culture is usually not an immediate event. Instead, it builds over time, accompanied by numerous causes and indicators.

Auditors need to stop the frantic pace of simply completing audit projects and consider what they observe in the different cultures present in their organization. Soft evidence on culture is not captured on a single audit, in a single way, through a single process. But when cumulative evidence is aggregated, internal auditors should have enough evidence to assess culture. They just need sufficient experience, understanding, perspective, and potentially courage to pull it all together and determine what it means. That is the nature of auditing culture. Ia

DOUGLAS J. ANDERSON, CIA, CRMA, *is managing director of CAE Solutions, Professional and Stakeholder Relations, at The IIA in Lake Mary, Fla.*

Auditing Analytic Models

Allan Sammy

Internal auditors need to assess the analytics controls for the models their organizations rely on to support decision-making.

The analytics gold rush is on. Organizations around the world are spending considerable money to build or buy analytic models and analytics capability to take advantage of big data, machine learning, and artificial intelligence (AI) technologies. These models have made their way into every aspect of business and are being relied on as decision support—and, in the case of machine learning and AI, actually making the decisions—for issues such as:

- Determining the probability of default for potential borrowers (corporate and individual).
- Evaluating new employees' probability of success and tenure with the organization (from professional athletes to salespeople).
- Forecasting success and return on investment for new marketing initiatives.
- Making product mix and store location decisions.
- And coming soon, making life-and-death decisions in self-driving vehicles.

Today's organizations have billions of dollars riding on the accuracy and performance integrity of analytic models. With model performance becoming a strategic enabler, organizations need to manage the risks associated with analytics.

To effectively manage these risks and move beyond simple financial model or spreadsheet auditing, organizations need a system of controls around analytic model development, application, and maintenance. These analytics controls provide checks and balances around model selection, validation, implementation, and maintenance. Periodic internal audits can help determine whether analytics controls are designed appropriately and operating effectively.

MODELS AND CONTROLS

An analytic model is a mathematical equation that takes in data and produces a calculation such as a score, ranking, classification, or prediction. It is a very specific set of instructions for analyzing data to deliver a particular kind of result—behavior, decision, action, or cause—to support a business process.

The objective of analytics controls is to ensure that:

- Analytics personnel have the appropriate skills and training.
- Input data is appropriate, complete, authorized, and correct.
- Model selection procedures are documented and justified.
- Model validation and testing have been conducted in accordance with scientific principles.
- Outputs are accurate, complete, and being used by the business as intended.
- The model is refreshed and reevaluated periodically.
- The organization maintains a record to track the processing of data from input, to processing, to the eventual output.

There are several types of analytics controls. *Skills controls* provide assurance that data analytics personnel are competent and sufficiently trained in relevant analytics methods. *Business-use controls* provide assurance that the model addresses the intended business objective. *Data controls* are used mainly to check the integrity of data entered into an analytic model. *Model selection controls* ensure model selection is appropriate and reasonable to provide decision support. *Model validation controls* address what is done to ensure the model output is reasonable and accurately reflects the underlying nature of the input data. *Output controls* provide assurance that the model output is presented and used in an appropriate and justified manner to ensure it remains consistent and correct. *Maintenance controls* address the need to reevaluate and refresh analytic models periodically to ensure they are still relevant in the current environment.

ANALYTICS VS. IT GENERAL CONTROLS

Internal auditors need to understand the relationship and difference between analytics controls and IT general controls. Otherwise, an analytics controls review may not be scoped appropriately, negatively impacting the audit's quality and coverage.

IT general controls apply to all systems components, processes, and data present in an organization or systems environment. The objectives of these controls are to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations.

Analytics controls differ from IT general controls because they relate to the methodology and data pertaining to each analytic model. They are specific to each individual application.

Internal auditors must note the degree to which management can rely on analytics controls for risk management. This reliance depends in part on the design and operating effectiveness of the IT general controls. If these controls are not implemented or operating effectively, the effectiveness of analytics controls is greatly diminished. For example, if the IT general controls that monitor program changes are not effective, then unauthorized, unapproved, and untested changes to an analytic model can be introduced to the production environment, thereby compromising the overall integrity of the model.

ASSESSING MODEL RISK

The example below of an analytic model control risk assessment uses a qualitative ranking scale (1=low impact or risk and 5=high impact or risk). Composite scores for each model are calculated by multiplying each risk factor and its weight in the model

ANALYTIC MODEL RISK FACTOR WEIGHTING

	20	10	10
Model	Model Supports Regulatory Requirement	Degree of Model Complexity	Prepackaged or Developed
Direct mail	5	1	5
Game mix	1	1	2
Lottery win	5	2	2
Anti-money laundering	5	3	5
Workforce	5	1	1

38% of internal audit functions that perform data analytics use it for most audits, according to Protiviti's 2018 Internal Audit Capabilities and Needs Survey.

ANALYTIC MODEL CATEGORIES

There are three main categories of analytic models: descriptive, predictive, and prescriptive. Each category can provide an organization value and strategic insight.

Descriptive These models allow organizations to condense big data into smaller, more digestible pieces of information. Typically, organizations that use analytics meaningfully have mountains of raw data at their disposal. Descriptive analytics enables an organization to summarize that data and determine what really happened. Most analytics in use are descriptive: sales breakdowns, social media likes and followers, ratings, and reviews.

Predictive The next level up in data analysis, predictive analytics uses a variety of statistical, modeling, data mining, and machine learning techniques to study recent and historical data, enabling analysts to identify patterns and correlations in the data. Based on these identified patterns and correlations, analysts can create a model of the future results given selected inputs. For example, based on certain borrower characteristics, a bank may use a predictive model to forecast its amount of loan defaults.

Prescriptive The highest level of analytics, prescriptive analytics recommends one or more courses of action and shows the likely outcome of each decision. Unlike a predictive model, a prescriptive model shows multiple future scenarios based on a decision the organization makes today. Prescriptive analytics requires a predictive model with two additional components: actionable data and a feedback system that tracks the outcome produced by the action taken. An example of prescriptive analytics would be a casino

MORE

VISIT InternalAuditor.org to read "Analytic Model Controls and Tests."

and adding the totals. For example, the composite score of 375 on the first line is computed by multiplying the risk factor rating times the specific model rating [(20 x 5) + (10 x 1) + (10 x 5) +...].

For this example, the internal auditor of a gaming company may determine that the analytic model control review will include all models with a score of 200 or greater.

	10	10	10	15	15	
	Model Supports More Than One Critical Business Process	Type of Data Processed by the Model	When Model Was Last Refreshed	Financial Impact	Effectiveness of the IT General Controls	Composite Score
	5	3	3	5	2	375
	1	1	1	4	2	170
	1	5	1	1	1	240
	1	5	5	5	2	395
	1	1	1	3	2	225

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

floor product mix optimization model that predicts revenue gains given various game configurations.

RISK ASSESSMENT

Auditors should use risk assessment techniques to identify critical vulnerabilities pertaining to the organization's reporting and operational and compliance requirements when developing the risk assessment review plan. These techniques include the review's nature, timing, and extent; critical business functions supported by analytic models; and the extent of time and resources to be expended on the review.

To add value to organizationwide analytics control risk assessment activities, internal auditors should define the universe of analytic models and supporting technology (modeling software, data services, etc.). They also should summarize the risk and controls using the risk and control matrices documented during the risk assessment process.

> Internal audit should determine the right scale for ranking each application control risk.

Next, internal auditors should define the risk factors associated with each analytic model by answering questions such as:

- Does the model support a regulatory requirement?
- How complex is the model type?
- How effective is the design of analytics controls?
- Is the model prepackaged (off the shelf) and customized or developed in house?
- Does the model support more than one critical business process?
- How is the data processed by the model classified (e.g., financial, private, or confidential)?
- How frequently are changes made to the model?
- How complex are those changes?
- What is the model's financial impact?
- How effective are the IT general controls residing within the application (e.g., change management, logical security, and operational controls)?

Once they have answered these questions, internal auditors should weigh all risk factors to determine which risks need to be weighed more heavily than others (see "Assessing Model Risk" on page 52). From there, they should determine the right scale for ranking each application control risk by considering qualitative and quantitative scales, such as:

- Low, medium, or high control risk.
- Numeric scales based on qualitative information (e.g., 1=low-impact risk, 5=high-impact risk; 1=strong control, 5=inadequate control).
- Numeric scales based on quantitative information (e.g., 1=less than $50,000 and 5=more than $1 million).

With this information in hand, internal auditors should conduct the risk assessment, rank all risk areas, and evaluate the risk assessment results. Finally, they should create a risk review plan that is based on the risk assessment and ranked risk areas.

AUDIT METHODOLOGY

Internal auditors should keep in mind that the review's scope, depth, approach, and frequency depend on the results of the risk assessment and the availability of internal audit resources. If the analytics team uses a recognized methodology for model development such as the

13% of internal audit functions surveyed are using analytics to identify risk and determine audit scope and planning, according to the 2018 PwC State of the Internal Audit Profession report.

Cross-Industry Standard Process for Data Mining (CRISP-DM) or some other widely accepted system, then internal auditors should consider auditing to that standard. In addition, some organizations have established a model risk management function. Internal audit can audit that area using similar methodology to that applied to other compliance functions.

For organizations whose analytics teams do not use a prescribed model development methodology, there are two approaches auditors can use to audit analytics controls: the Integrated Model Review Methodology (IMRM) and the Stand Alone Model Methodology (SAMM). These methods apply CRISP-DM principles in an internal audit context.

IMRM This approach can be used to evaluate model risk by examining all the business processes that feed or are dependent on the model being reviewed. When using the IMRM, internal auditors should include within the review's scope all the organization's systems that are involved in the model under review and whether the implementation of the model is consistent with the organization's analytics strategy. In other words, the auditor needs to include within the review's scope the separate processes that make up the different components of the model cycle. The auditor then can identify the inbound and outbound interfaces within the model and complete the scoping activity. For example, when auditors review a marketing campaign response model, they would scope in survey methodology and data collection processes, customer segmentation processes (inputs), and marketing decisions made based on model output.

Using the IMRM approach automatically devotes more audit resources to those analytic models that affect a larger portion of the organization's operations. To use the IMRM effectively, auditors need to understand the business processes surrounding the use of the model being reviewed and how data flows into and out of the model.

SAMM The alternative approach, the SAMM, is used when the auditor wants to review the controls within a single model. The SAMM is useful for new models or when audit resources are limited. Essentially, the auditor is verifying that the model, itself, has appropriate controls and performs the intended function. It does not provide assurance as to whether the organization is using the model output effectively or whether the model inputs are valid. Although SAMM is effectively a subset of the IMRM, internal auditors should clearly specify which methodology they are applying so that management and the audit committee know the extent to which they can rely on the results.

> **The auditor needs to include within the review's scope the different components of the model cycle.**

IT'S STILL INTERNAL AUDITING

Although many auditors may be unfamiliar with analytic models, machine learning, and AI, the fundamentals of internal auditing remain the same. As with all new technologies and processes that organizations have embraced, internal auditors have a responsibility to learn how analytic models can be useful in their work and adapt their methods to serve their stakeholders. Ia

ALLAN SAMMY, CIA, CPA, CGA, *is director, Data Science and Audit Analytics, at Canada Post in Ottawa.*

BY KELLEY ELLIS EDITED BY KAYLA FLANDERS

MODEL GOVERNANCE, WHERE TO BEGIN?

Internal audit should periodically review the governance structure and related sub-process responsibilities.

Models serve many purposes and support various decisions across an organization. A model is a mathematical representation of an entity system given certain operational, financial, compliance, and/or economic conditions that aims to quantify past, present, or future outcomes to provide decision-making information. Models typically are used to predict future results or to allow an entity to perform analysis within the mathematical model to determine the impacts of different drivers or variables on model output. Models can be simple calculations in an Excel spreadsheet with a small table of variable inputs, or they can be highly complex mathematical and statistical computations with a web of interrelated models using sophisticated software on a dedicated server.

Model governance provides oversight and control to minimize model risk, establishes policy to protect the integrity of the model output used in decision-making, prioritizes and authorizes changes to models used by the organization, and facilitates the sharing of information across the organization regarding the use and limitations of the models to improve transparency.

Before internal audit can evaluate the model governance structure and effectiveness, it needs to gain an understanding of the models that are used within the organization. This can be time-consuming. Documentation is valuable to any process, but it is difficult to find in practice. Internal audit may have to work with management to develop an initial listing that can be used to identify and assess risks and determine the audit scope. The list of models should include:

- Name for the model.
- A brief description of the model's purpose and use.
- Key model personnel: model owner, developer, tester/validator, production operator, and users.
- Frequency of model output reporting.
- The software and platform used for the model.
- The latest version of the model being used.
- The model risk rating.

The model owner should maintain more detailed information for each model regarding inputs, assumptions, methodologies, process documentation with risks and controls identified, data flow diagrams, items excluded from the model, approximations or assumptions used in the model, model limitations, manual outside adjustments to the model, and software and hardware used by the model.

The model risk rating should be based on probability and impact and be consistent with other risk rating structures used within the organization. When determining the model risk rating, internal audit should consider several risk drivers

READ MORE ON GOVERNANCE Visit InternalAuditor.org/governance

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

MODEL GOVERNANCE COMMITTEE RESPONSIBILITIES

Potential responsibilities may be completed by the committee, management or a project team with committee oversight, or some combination thereof. Responsibilities will vary but could include:

- Develop, approve, and communicate model policy, standards, and procedures.
- Plan resources and prioritize tasks when there are competing priorities or dependencies.
- Review and approve technical papers from subject-matter experts regarding gray areas or where there is disagreement on model approaches.
- Prioritize and approve model changes, including tolerance and materiality levels for approvals needed for model changes.
- Review and approve risk control matrices for material models. Also, have insight into control issues that impact the model, including general IT and application controls over inputs, processes, and outputs.
- Monitor compliance issues that impact the model and approve management actions to remediate issues.
- Oversee model data quality – integrity; outliers; timeliness and availability; security; and extraction, transfer, and loading.
- Oversee model validation – static and dynamic testing, sensitivity analysis, analytics, user acceptance testing, analysis and quantification of changes, and identification of risk-based deep dives into current models on an ad hoc, periodic, or rotational basis.
- Provide an objective, robust check and challenge process on model results.
- Approve outside-the-model adjustments and rationale for use.
- Maintain a list of known model limitations and implications for use.
- Approve the timing of model releases to production.
- Coordinate the reporting calendar and use of model results.
- Identify stress and scenario testing for the models and determine management actions.
- Provide a consistent, common communication point to address questions and drive improvement.

(along with other relevant criteria based on the industry or business), including: financial statement impact of results, level of model dependency in making business decisions, regulatory requirements, complexity of calculations and the extraction/transferring/loading of inputs, degree of interdependencies among models, subjectivity of assumptions or inputs, experience level of the personnel involved, historical experience of issues, effectiveness of controls, and degree of incentive compensation that may be tied to performance or output.

Once the listing of models is compiled, risk rated, and agreed upon by key stakeholders, internal audit can perform an assessment of model governance focusing on the high-risk models as a starting point. All high-risk rated models should be within the purview of a model governance committee.

The scope of responsibilities of a model governance committee is subject to debate and tends to be the victim of scope creep given the volume of risks associated with models. "Model Governance Committee Responsibilities" on this page provides a comprehensive listing of items to be considered in determining the scope of a committee. There may be other responsibilities specific to an organization or evolving risks.

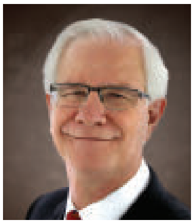
The structure and oversight of the model governance committee should be tailored to the specific needs and level of maturity of the organization:

- The committee should report to the board directly, or indirectly via another committee.
- Membership should include a variety of senior-level model stakeholders.
- Responsibilities should be clearly defined for committee members and those involved in the modeling process.
- Committee decisions should be clearly documented with supporting rationale in committee minutes.
- A communication process should be in place to notify those who are responsible for any follow-up actions, noting anyone who should be consulted or informed.

Having a model governance committee centralizes the identification of, and response to, model risks, which typically improves communication across stakeholders, builds consensus around decisions, establishes controls, and enables management action given the diversity of committee membership. The focus on model risks by regulators and external auditors has been increasing. Having a committee that receives and generates appropriate documentation makes it much easier to address those concerns. Ia

KELLEY ELLIS, CIA, CPA, CGMA, FLMI, *is assistant professor of practice, and assistant director, School of Accounting, Drake University, in Des Moines, Iowa.*

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



BY J. MICHAEL JACKA

"TRUST ME," SAID THE SMILING AUDITOR

To succeed as advisors, we need to understand what truly inspires confidence from stakeholders.

Buzzwords are fascinating creatures. They stampede their way into the lexicon like cavalry to the rescue, bludgeon us with constant overuse, and then become reviled as trite clichés used in lieu of actual thought. But closer examination reveals that buzzwords achieve their status because, at some point, they perfectly articulated some important concept. *Empowered, synergy, bleeding edge, think outside the box*—once meaningful concepts, they have become little more than collections of nonsense syllables.

Internal auditors are not immune. We are currently overusing an important phrase that, if we are not careful, will lose its power and be summarily dismissed into buzzword oblivion. And that would be a shame, because the phrase *trusted advisor* is extremely powerful.

Becoming a trusted advisor is a worthy aspiration. But the phrase risks becoming a hackneyed cliché because auditors have quit thinking about what the phrase really means. Sure, they understand the concept of *advisor*, but they lose sight of the key concept—*trusted.*

As IIA President and CEO Richard Chambers notes in his appropriately titled book *Trusted Advisors,* "trust is one of the most underused words in the internal audit vocabulary. … Rarely do we speak of whether [our stakeholders] should trust us."

Many auditors think that if they work on their relationship management skills and try to tell the truth, trust will follow. But trust is much more than building rapport and managing relationships.

Trust comes from actions, not words. It is what others see us do, what others discover we have done, and what others believe we will do. It comes from something as simple as meeting our agreed upon deadlines, and from something as complicated as having the integrity to report what is rather than what everyone wants to hear. It represents the accumulation of activities that show we either back what we say or turn our backs on our promises, our clients, and ourselves.

Years ago I worked with an executive who I had known since we were both lowly supervisors. On one occasion, internal audit discussed the results of an audit with him and one of his directors, and the director argued every one of our points. Finally, the executive said, "I have worked with internal audit for years. If they say there is a problem, then there is a problem. I don't want to hear excuses; I want to hear how you are going to fix this."

Still, gaining clients' trust in audit work is only table stakes. Do clients trust your advice? That's a nice start. Do they trust you to be a part of the management and leadership team? Much better. Do they trust you enough to turn to you for advice every time something important is happening, confident that you will provide objective and independent information that will aid decision-making? If so, then you are truly a trusted advisor.

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

DISRUPTIVE BUSINESS

Internal auditors need to keep a finger on the pulse of change and advise their organizations accordingly.

LISA HARTKOPF
Partner
EY

RICK SHRINER
Principal
RSM

What are the disruptions facing today's businesses?

HARTKOPF In today's transformative age, businesses are being disrupted from every angle. With changes to global laws and regulations, organizations are challenged to rethink how they comply. In addition, volatility in the global economy may be impacting companies' bottom lines. Paired with these shifts, sectors are also converging at lightning speed—creating new risks and opportunities for businesses in every industry. In the global digital world, digitally enabled companies have a competitive advantage over traditional industry incumbents. As companies move into new sectors and digitally native businesses dominate, acquisitions and divestitures are reshaping the focus and makeup of businesses. Big data is moving beyond being just a buzzword, and business leaders are using data to drive competitive insights and make big moves. Even the consumer is changing. With more access to information and the internet at everyone's fingertips, preferences and expectations are not what they used to be.

SHRINER Businesses are facing more fundamental uncertainty than at any time since World War II. Technology and automation are reshaping and, in some cases, replacing jobs in customer service, and with the advent of artificial intelligence (AI), even roles that require decision-making skills are under threat. The nine-to-five model, itself, is being challenged by the gig economy, with work "paid by the hour" replacing the daily effort of the long-tenured employee. The knowledge worker is being replaced by the data worker, developing and feeding the algorithms that make the predictions that drive an increasing number of daily experiences. Meanwhile, a war for data is being waged, with the spotlight on social media and technology companies. The internet's long memory of user interests—cookies—and the companies that monetize personal information are being challenged by the "right to be forgotten" and other data protection principles from regulators and from a concerned public. This war will intensify and be waged across countries with different social norms and legal frameworks. Within this environment, managers must motivate and direct, deliver products and services, and make plans for the future.

What are the risks posed by disruption?

SHRINER All businesses run the risk of failing to define and respond to competitive pressures or market needs. The dominance of technology mega companies will keep many established industries on their toes. Who thought that an e-commerce company would buy a premium grocery store chain? Further, an increasingly mobile workforce in a tight labor market means

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

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

less innovative companies may be starved – or bled – of high performers with next-generation skills. In many respects, business disruption is a war for talent.

HARTKOPF It's important for businesses to continue to change and constantly innovate. Maintaining a status quo business model without regard for external influences—legal/regulatory, competitor, economic, technological—will put businesses at a disadvantage in the marketplace and potentially result in losses or penalties. Organizations that do not embrace new technologies—AI, robotics—will not be able to compete in the global digital environment. The additional challenge is that these new technologies may create an even larger talent gap as existing employees may not be best positioned to address them. It's important for companies to understand the potential impact of these risks and the influence of other external forces as they could negatively affect business outcomes.

How can organizations prepare for the new ways of working that go with business transformation?

HARTKOPF Organizations need to constantly update their strategic objectives and communicate them broadly. Embracing new technology can be a first step in transforming your business model, driving growth, and increasing efficiency. At the core of this transformation is the need to stay true to your business objectives, increase the company's agility, and establish a flexible model to help facilitate quick responses to external shifts. Perhaps the best way to prepare for new thinking is by tapping the right people for your business. Organizations need to place an emphasis on not only attracting, retaining, and advancing diverse talent, but also adopting a flexible workforce model that enables a business to engage the right resources, at the right time, and in the right place.

SHRINER Going on the offensive begins with understanding where your operations might be vulnerable. Companies are identifying specific areas of excessive complexity, lag, or cost in their operations, be it in supply chains, sales channels, customer engagement models, or back-office processes. Doing so gives organizations a glimpse of where operations may be most impacted by disruption—positively or negatively—and enables an evaluation of responses. But that's only part of it; companies will require great vision, adaptability, and commitment to allocate key talent and resources at the expense of shorter term value. Most companies are viewing these modernization efforts as a multiyear journey.

How can internal audit be involved in efforts to address disruption?

SHRINER Internal audit needs to be involved in its company's commercial activities, which will be most impacted by disruption from new regulations, technologies, or competitors. For example, helping navigate new data privacy law implications of acquired customer information is not only risk mitigating, but also incredibly helpful to the business' future acquisition strategy. Internal audit needs to ask itself, "Are we close enough to the sources of disruption?" Second, given the impacts of disruptive technologies will be profound, many internal auditors aren't waiting around to be surprised by the changes. They are talking to AI, automation, and data visualization companies now, often piloting the technologies, themselves, and facilitating business adoption along the way. Little of this happens, however, without an accommodative company culture.

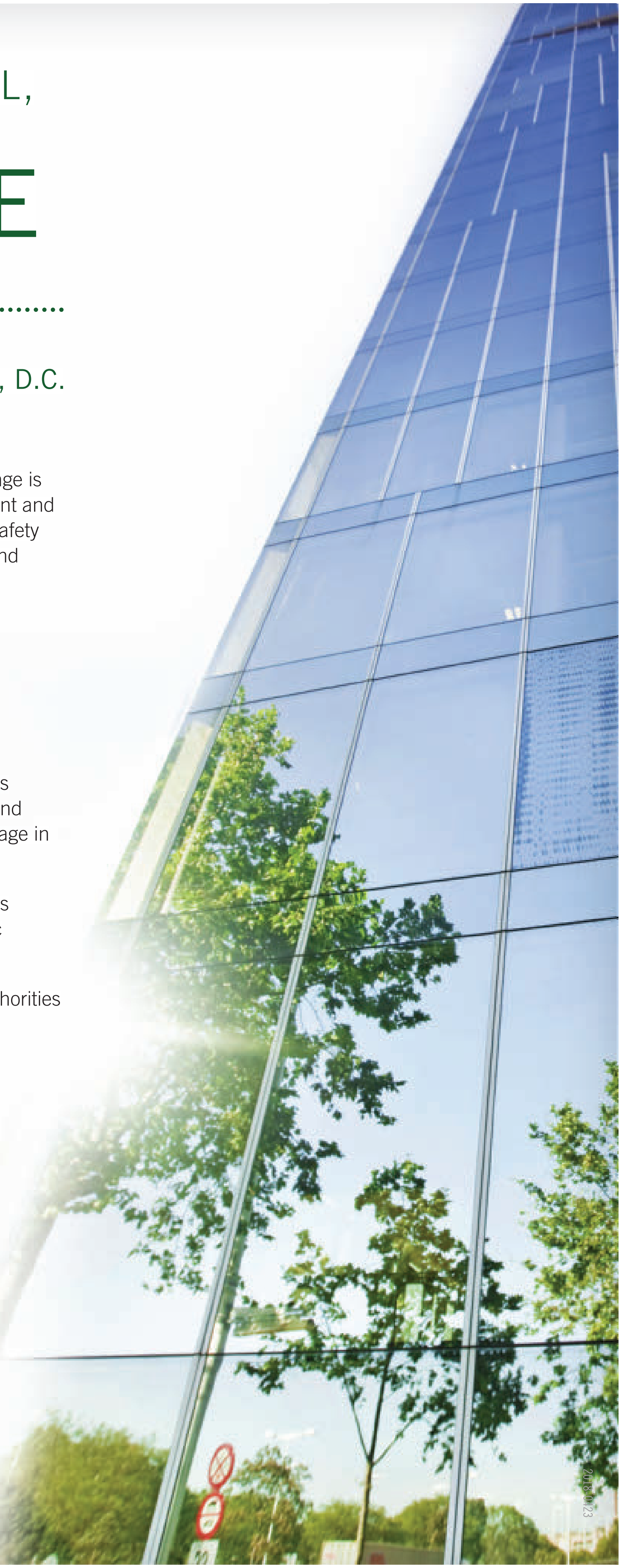
HARTKOPF Internal audit is in a unique position to address and facilitate business disruption. The team should be actively involved in discussions concerning the organization's strategic plan—including objectives around strategic transactions such as acquisitions, divestitures, major system implementations, joint ventures, and alliances. In driving an organization forward, internal audit can coordinate frequent enterprise risk assessments to stay ahead of external forces and provide timely insights developed during reviews that focus on emerging risks. Internal audit should keep a finger on the pulse of changes occurring in the marketplace and conduct benchmarking to help management anticipate the impact on the organization.

Does internal audit need to disrupt or transform itself?

HARTKOPF Internal audit has been "transforming" incrementally over the last 20 years, but these changes haven't been disruptive. To keep pace with the changes affecting the business and provide forward-looking insights, internal audit will need to make some overarching changes, including:

- Redesigning the operating model to be more flexible, timely, and focused on the risks that matter.
- Understanding and embracing new technologies.
- Tapping a flexible workforce model to deliver the most appropriate knowledge, experience, and skills.
- Coordinating more effectively with the first and second lines of defense by having them embrace responsibility for initial validation and control monitoring, respectively.

SHRINER Let's face it: The business of internal audit is being disrupted in much the same way as companies overall. The next five years will present more change to our profession than did the past 15 years. Hints of those changes are evident today. For example, it's common to see internal audit functions comprising 10 percent to 20 percent "data people" in addition to accountants or IT specialists. These percentages will increase. The tools of our trade are rapidly evolving. It may not be long before data visualization tools eclipse PowerPoint for communicating audit results. Auditors will need to learn to detect process deviations or control issues from the output of automation tools or bot algorithms. Ia



IIA Calendar

IIA CONFERENCES
www.theiia.org/conferences

AUG. 13–15
Governance, Risk & Control Conference
Omni Hotel
Nashville, TN

OCT. 1–2
Financial Services Exchange
Renaissance Downtown
Washington, D.C.

OCT. 3
Women in Internal Audit Leadership Forum
Renaissance Downtown
Washington, D.C.

OCT. 3–4
Environmental, Health & Safety Exchange
Renaissance Downtown
Washington, D.C.

OCT. 21
Emerging Leaders
Aria Resort & Casino
Las Vegas

OCT. 22–24
All Star Conference
Aria Resort & Casino
Las Vegas

OCT. 24–25
Gaming & Hospitality Conference
Aria Resort & Casino
Las Vegas

IIA TRAINING
www.theiia.org/training

JUNE 4–22
CIA Learning System Comprehensive Instructor-led Course – Part 1
Online

JUNE 5–8
Various Courses
Dallas

JUNE 5–14
Assessing Risk: Ensuring Internal Audit's Value
Online

JUNE 5–28
CIA Learning System Comprehensive Instructor-led Course – Part 2
Online

JUNE 12–15
Various Courses
Las Vegas

JUNE 18–27
The Effective Auditor – Understanding and Applying Emotional Intelligence
Online

JUNE 19–22
Vision University
Philadelphia

JUNE 19–28
Enterprise Risk Management: A Driver for Organizational Success
Online

JUNE 26–27
Data Analysis for Internal Auditors
Online

JUNE 26–29
Various Courses
Denver

JUNE 29
Fundamentals of Internal Auditing
Online

JULY 9–18
Fundamentals of IT Auditing
Online

JULY 9–18
Performing an Effective Quality Assessment
Online

JULY 10–19
Risk-based Auditing: A Value-add Proposition
Online

JULY 17–20
Various Courses
Orlando

JULY 17–26
Operational Auditing: Influencing Positive Change
Online

JULY 18
Fundamentals of Internal Auditing
Online

JULY 23–25
Leveraging and Influencing Millennials and Other Generations
Online

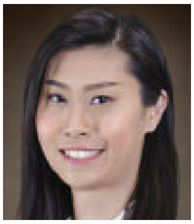
JULY 24–27
Tools & Techniques II: Lead Auditor
Kansas City, MO

JULY 30–31
IT General Controls
Online

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 grace.wu@theiia.org



BY JINGWEN (GRACE) WU

RISKS SPEAK LOUDER THAN ISSUES

Internal audit communication should focus on the key threats our clients face.

Mutual understanding between internal audit and its clients can be difficult to achieve. When audit clients hear jargon such as "issues" and "gaps," or read it in an audit report, they often stop listening. They're left with the impression that internal audit doesn't understand the risks their area faces and that its reporting is irrelevant. At the same time, auditors may experience frustration over clients' failure to understand audit issues. Why can't issue communication be easier and more effective? In many cases, it's because auditors don't "speak the same language" as their clients and fail to communicate adequately about risk.

The IIA Position Paper, The Three Lines of Defense in Effective Risk Management and Control, states that risk management and control duties must be coordinated carefully organizationwide "to assure that risk and control processes operate as intended." In reality, that coordination does not always happen. For the first-line business units conducting day-to-day operations, if there are no risks within the immediate processes they manage, there are no issues. At the same time, many internal auditors perform their work in isolation, targeting check boxes without comprehensive understanding of risks, even though second-line risk management and compliance functions are looking at risk appetite and the risk landscape enterprisewide. Effective risk communication can be challenging when internal auditors are out of sync with other assurance providers and adhere to an outdated, myopic approach.

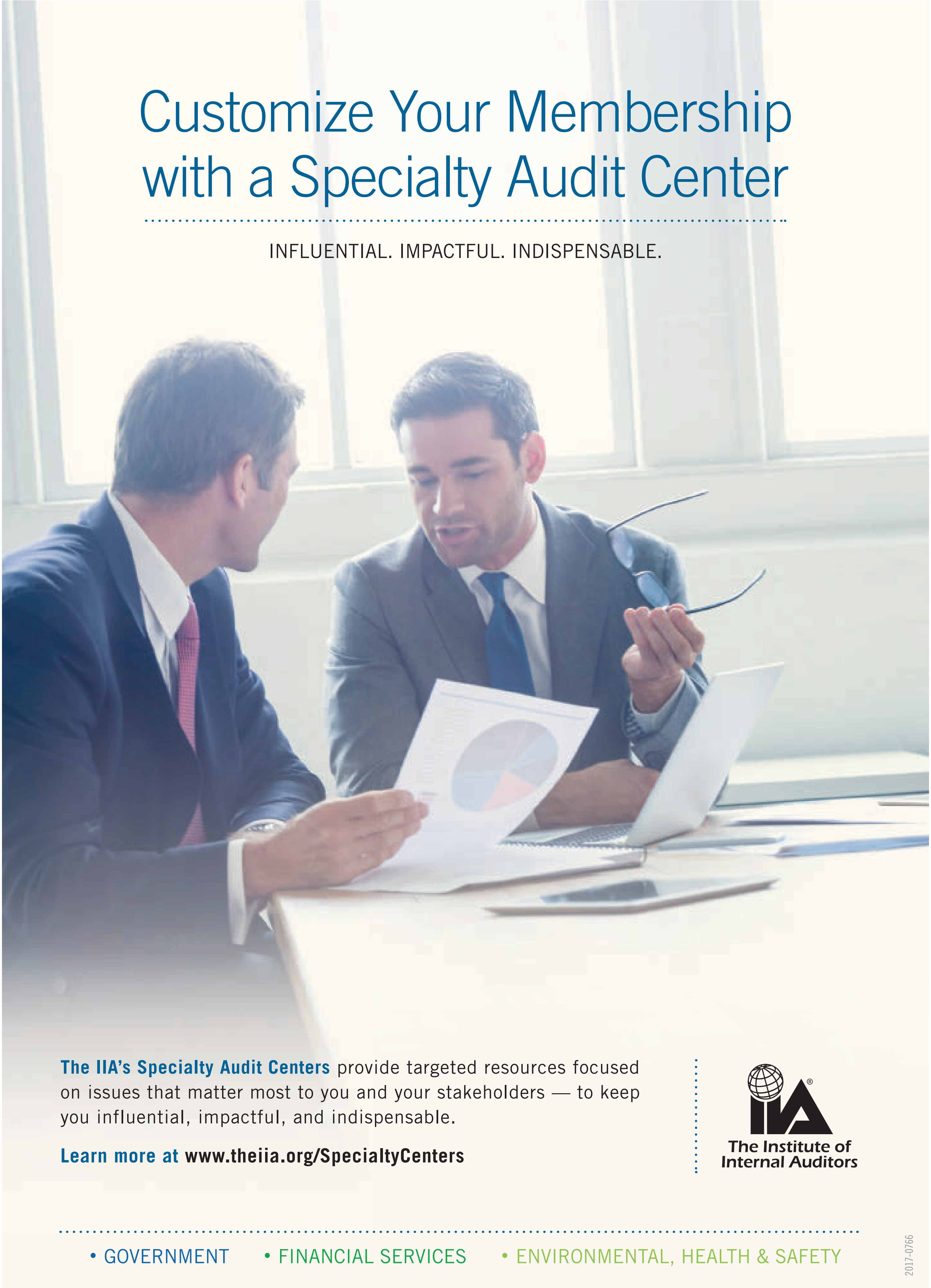
In today's rapidly changing environment, the traditional method of identifying issues simply based on test results for design and operational effectiveness constitutes an insufficient means of risk analysis, reporting, and acceptance. Although test results provide a solid basis for showing how the client failed, they don't provide much insight into why clients should care other than a low score. And if our deliverables lose relevance to the audience, we lose buy-in.

Within the audit report, risk-based information tends to be underdeveloped and fails to provide adequate support for issues. Risk statements often appear merely as a single line in each issue table, and risk analysis may not be presented holistically anywhere in the report. Moreover, risk assessment usually occurs during the planning and scoping phase of an audit. Even if the assessment has been performed well and reveals areas of weakness, key risk indicators would be gradually lost during an audit and toward the conclusion of the engagement, leading to unclear answers about true risk. Risk conversations should instead take place throughout the entire audit.

Before presenting issues to clients, internal auditors should ask, "Did I perform sufficient risk analysis to cover significant areas?" rather than "Have I identified enough findings?" Overall, the goal of issue communication should not be putting down names on the sign-off sheet, but rather mutual agreement on risks and a willingness to address them. Ia

JINGWEN (GRACE) WU, CIA, *is compliance officer, Risk & Governance, at Silicon Valley Bank in Santa Clara, Calif.*

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


Customize Your Membership with a Specialty Audit Center
INFLUENTIAL. IMPACTFUL. INDISPENSABLE.
The IIA's Specialty Audit Centers provide targeted resources focused on issues that matter most to you and your stakeholders — to keep you influential, impactful, and indispensable.
Learn more at www.theiia.org/SpecialtyCenters
The Institute of Internal Auditors
• GOVERNMENT
• FINANCIAL SERVICES
• ENVIRONMENTAL, HEALTH & SAFETY
2017-0766