Ia INTERNAL AUDITOR

APRIL 2019

A PUBLICATION OF THE IIA

A Look at Risk's Upside

Smart Cities Present Steep Audit Challenges

Keep Your Focus on the Client

Navigating Stakeholder Expectations

GDPR's GLOBAL REACH

The philosophy underlying Europe's data privacy law is finding its way into regulations around the world.

Ia
INTERNAL AUDITOR

APRIL 2019 VOLUME LXXVI: II

FEATURES

Ia
INTERNAL AUDITOR

APRIL 2019 VOLUME LXXVI: II

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Banks and Bitcoin JPMorgan Chase's recent decision to offer its own digital coin could help cryptocurrency gain more traction in the traditional financial system.

Audit Reporting Do's and Don'ts What separates relevant audit reports from those that fall by the wayside? Watch a series of videos on reporting pitfalls and best practices.

Big Scam on Campus CEOs and celebrities are among parents accused of bribery and cheating to get their children accepted at elite universities.

GAM 2019 Read our coverage of The IIA's General Audit Management Conference, with topics ranging from change and disruption to leadership and innovation.

Find us on Facebook

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. Copyright © 2019 The Institute of Internal Auditors Inc. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Lake Mary, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

COVER AND PREVIOUS PAGE: ILLUSTRATION BY SEAN YATES, BASE PHOTOGRAPH BY VIKTORUS/SHUTTERSTOCK.COM; THIS PAGE, TOP: AGSANDREW / SHUTTERSTOCK.COM, BOTTOM: 3DSCULPTOR / SHUTTERSTOCK.COM

EMERGING LEADERS 2019

Who Are Internal Auditing's 2019 Emerging Leaders?

What defines an **extraordinary** internal auditor?

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

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

Nominate by May 10, 2019
at **www.InternalAuditor.org**.

EMERGING LEADERS 2018

ALEX HARDY
CIA, CA
30
ASSOCIATE DIRECTOR, AUDIT & ADVISORY
PROSPERITY ADVISERS GROUP
NEWCASTLE & SYDNEY, AUSTRALIA

ALEX HARDY has big ambitions, and one of them is helping young professionals move forward in their careers. "His ambition to attain a partnership role at the company is guided by his vision of transforming the firm's audit practice and capitalizing on technological opportunities," says colleague Stephen Coates, a director at Prosperity Advisers Group. But Hardy's proudest achievement, Coates adds, is being a mentor to junior staff. Already, Hardy is a founding member of the company's Employee Advisory Board and, beyond the firm, he was named to the inaugural IIA–Australia Youth Leadership Committee. The University of Newcastle graduate is also executive director at Hunter Young Professionals, which provides opportunities for young people to network in a business environment. Indeed, says Bryant Richards, associate professor of accounting and finance at Nichols College and one of this year's Emerging Leaders judges, "No longer emerging, this individual is a current leader of the profession." Hardy presents weekly to boards, shareholders, and management on audit outcomes and opportunities for improvement. And he provides pro bono professional services to Renew Newcastle, Cooks Hill Surf Lifesaving Club, and Ronald McDonald House. He also talks a lot about technology. "If you don't know what blockchain, AI, big data, and real-time access mean, then you are already behind the eight ball," Hardy says. "All of them are game changers, and a degree of fluency is important for future success."

ROBIN NOACK
CIA, CPA
29
AUDIT MANAGER
FEDERAL HOME LOAN BANK OF PITTSBURGH
PITTSBURGH

ROBIN NOACK understands that effective internal audit demands interaction with other areas of the business. The Pennsylvania State University graduate made a concerted effort to learn Federal Home Loan Bank of Pittsburgh's new governance, risk, and compliance application—and ultimately developed many of the ways the internal audit department puts it to use, notes colleague Dawna Fisher, senior manager at Federal Home Loan Bank. "She also developed a strategy for optimizing interactions with other departments to ensure identification of business unit risks and controls is complete and accurate," she says. Noack's strategy—established by coordinating with other lines of defense within the bank and working closely with the business units—enables internal audit to track audit-related issues that need validation and provide the follow-up on them that regulators require. Her team also prioritizes in-person interaction with clients. "We make every effort to socialize throughout the bank, building trust and positive relationships," Noack says. Business unit leaders regularly request her insights on hot topics and emerging risks in the financial services sector. Noack says knowing the business is part of the job. "It would be impossible to effec

"IT WOULD BE IMPOSSIBLE TO EFFECTIVELY
WITHOUT AN INTIMATE UNDERSTANDING O
STRONG RELATIONSHIPS WITH THE PEOPL

26 INTERNAL AUDITOR

JUSTIN FINN
CIA
28
ASSISTANT VICE PRESIDENT, SENIOR AUDITOR
BANK OF AMERICA
PLANO, TEXAS

JUSTIN FINN is "the auditor of the future, possessing both audit and analytical skills," according to his supervisor, Jim McCole, senior vice president and audit director at Bank of America. Finn, a University of North Texas graduate, started out in the firm's straight-from-college Corporate Audit Analyst Program, picking up business audit skills in issue validation, point-in-time audits, regulator issues, and continuous audit work in his first rotation. And with no previous Structured Query Language (SQL) experience, he learned to execute automation work relating to data analytics, exception testing, and continuous monitoring testing in the rotation that followed. Finn now serves as instructor for Corporate Audit's SQL training program and as "automation sponsor" for the bank's Audit Automation Analytics Champion program. "For sure, technology and the way we understand data will lead things forward," Finn says. One example is data analytics and automation that enable full-population testing, eliminating the need for a sample approach, he says; another new technology that internal audit is adopting is artificial intelligence-driven ongoing monitoring that replaces some task work. Both require practitioners to develop new data analytic skills and delve beyond a superficial understanding of the technology. At Bank of America, Finn's internal audit department focuses on finding and extracting data to cre

LINH MAI is passionate about internal auditing and about sharing his knowledge of the profession. Indeed, The University of Texas (UT) at Dallas graduate served as the university's IIA/ISACA/ACFE student chapter president as an undergraduate and at the same time was a teaching assistant at UT Dallas' Center for Internal Auditing Excellence. He also became "the face of the UT Dallas Internal Auditing Education Partnership (IAEP) program," says Center director Joseph Mauriello. "As student coordinator, he worked with leading internal audit departments and professional services firms to introduce themselves to UT Dallas IAEP participants." Mai also organized student volunteer efforts for the IIA–Dallas Super Conferences and the UT Dallas Fraud Summit. He has since delivered numerous addresses to internal audit audiences on developing student organizations, and he volunteers with ISACA's North Texas Chapter. At EY, he leads audits on areas ranging from Sarbanes-Oxley compliance to cybersecurity. "Sometimes innovative thinking is a matter of thinking differently about an existing innovation," Mauriello says. "He accomplishes this through his advocacy efforts." Part of his message is the reality of the profession's role. "I had the impression that most companies, operations, and internal audit functions were mature," Mai says. "However, the reality is there is significant potential for audit functions to generate value by advising and consulting on improvements in business processes." He adds that he's inspired and motivated by the vast opportunities for internal audit to help stakeholders, especially with the aid of technology. "I envision more processes, such as internal controls over financial reporting, requiring less overhead while providing more useful data," Mai explains, "allowing internal audit a greater opportunity to become advisors and freeing them from strictly regulatory or compliance functions."

LINH MAI
CIA, CISA
27
SENIOR, IT RISK

INTERNAL AUDITOR 27

Ia
INTERNAL AUDITOR

OCTOBER 2018

A PUBLICATION OF THE IIA

10 Tips for Career Management

Applying COSO's ERM Principles

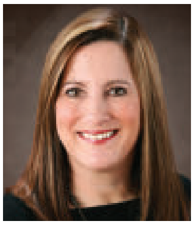
Audit's Role in Business Process Improvements

Advocating for the Profession

EMERGING LEADERS 2018

This year's standout practitioners exude talent and are passionate about promoting and enhancing internal auditing.

2019-2215



GDPR IS JUST THE BEGINNING

It is no surprise that cybersecurity and data protection remain top worries among chief audit executives (CAEs) responding to this year's IIA North American Pulse of Internal Audit report. Seventy percent are highly concerned about the potential for reputational harm stemming from an inappropriate disclosure of private data. What *is* surprising is that CAEs are far less concerned about compliance with new data protection rules. Nearly 50 percent of respondents say their organizations have minimal or no concern.

Almost a year after the European Union's General Data Protection Regulation (GDPR) went into effect, organizations are feeling "GDPR's Global Reach" (page 24). And, it's just the beginning. China has introduced regulations on cybersecurity, data protection, and cross-border data transfer that are reflective of GDPR. Brazil has a new General Data Protection Law that will go into effect in early 2020, and new and revised regulations are coming out of Australia and Japan, among many others. And, in the U.S., the California Consumer Privacy Act will take effect next year.

"Compliance requirements like GDPR are forcing changes in the way data is handled in many organizations," Jan Hertzberg, a privacy consultant, tells author Arthur Piper. "For CAEs, it is not just about data privacy, but data integrity throughout the business."

The many new data privacy regulations "highlight the need for organizations to get their data protection practices in order," says Pam Hrubey of Crowe in this issue's "Eye on Business" (page 64). Hrubey says organizations tend to have common challenges relating to data protection. She and Mike Maali of PwC consider those challenges and how organizations can safeguard information, as well as internal audit's role in privacy governance.

In the Pulse report, concern about GDPR compliance escalates in line with the size of the respondent's organization. In organizations with more than 50,000 employees, 62 percent rated compliance as a high concern compared to 29 percent who rated it that way overall. This suggests that larger organizations are more likely to have international operations. However, for others with international operations, there also could be some misunderstanding of when these new rules apply, as they are based not on the location of the organization, but on the location of the customer whose data is being gathered. To read the full 2019 Pulse report, visit http://bit.ly/pulse2019.

On another note, it's time once again to recognize high achievers in the profession. Nominations for *Internal Auditor*'s 2019 Emerging Leaders are now open. See the opposite page to learn how to nominate. Tell us who are the best and brightest in your internal audit functions and look for the article featuring this year's leaders in October.

Anne

@AMillage on Twitter

Reader Forum

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

Ia
INTERNAL AUDITOR
TRIALS AND TRANSFORMATION
Ten years after the global economic crisis, the internal audit profession is strong and ready to take on new challenges.
Richard F. Chambers, IIA president and CEO

Communication 101

The theme of this issue of *Internal Auditor* is Communication 101 for internal auditors and the chief audit executive. The majority of articles offer reminders and tips on communicating results to senior management. There was something for everyone, from the private sector to the government sector, to apply in fine tuning their communication skills while delivering audit results — and pointing out areas of risk to address. The key thing among all of the articles is ensuring that information is relevant and in plain language to allow better buy-in, so that internal audit is seen as an ally in helping the organization minimize risks and achieve its goals.

Frederick Lee comments on the February 2019 issue of Internal Auditor *magazine.*

The Future of Internal Audit

I am just beginning research on "The Future of Internal Auditing and the Development of New Technological Tools" as part of the dissertation for my master's in accounting. The interview is timely because, like IIA President and CEO Richard Chambers says, we are facing an era of digital revolution, and the internal auditor must maintain professional care and anticipate changes that may arise and affect the company. In addition, it is essential for today's auditor not to rest on his or her achievements. Internal audit must continue to develop its communication skills to inform these risks timely, thus maintaining a good relationship between shareholders and owners, and adding value to its role. I totally agree with Chambers when he says, "When you're busy looking behind, you lose what lies ahead."

Liz Alicea comments on Anne Millage's "Trials and Transformation" (February 2019).

Sidestepping Controls

I'm always interested in the contrast between "bottom-up" versus "top-down" fraud schemes. In this case, Grant Wahlstrom and Anisa Chowdhury described a similar fraud that was uncovered at a different location—presumably not connected to the primary culprit, Fogbottom. I think there are opportunities to focus attention on the susceptibility of certain controls to bottom-up circumvention to the point that it potentially becomes pattern abuse, similar to what a complexity scientist would call self-organized criticality.

Patrick McGowan comments on Grant Wahlstrom and Anisa Chowdhury's "The Phony Customer Fraud" ("Fraud Findings," February 2019).

Psychology Cross-training

Great short summary of the challenge. I conducted my first culture audit in 1999. At the time it was unheard of to even do

Ia
INTERNAL AUDITOR
APRIL 2019
VOLUME LXXVI:II

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design

PRODUCTION MANAGER
Gretchen Gorfine

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

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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

this. I had to cross-train in psychology, adult learning behaviors, and how to gather data that sits within people versus documents. The results of a culture audit shift organizations powerfully and in unimaginable ways over traditional audits. We now conduct compliance and culture audits that deliver powerful root causes beyond the compliance findings, empowering organizations to shift much faster than with just compliance audits. Every auditor should now cross-train into psychological and adult learning behaviors as this area will grow and grow.

Elizabeth Frische comments on Jim Roth's online series, "Auditing Culture: History and Principles" (InternalAuditor.org).

Challenging Business as Usual

This is a great video with some very real scenarios on how technology and leadership will shape internal audit going forward. I'm still not entirely sold on the use of the words *disruption* and *disruptive* to describe the concept of challenging business as usual, though. I always associate disruption with something bad, inconvenient, frustrating, intrusive, poor, and annoying. How else do people feel about this as a term and how would you sell anything "disruptive" to an audience that associates the term as a negative?

Darren Roberts comments on the video, "Disruption: Leadership Approach" (InternalAuditor.org).

What Do Internal Auditors Do?

The scope of internal audit can be so broad that it is difficult to succinctly articulate what the job entails. I have often found it helpful to sit back and consider this question periodically to ensure that internal audit activities continue to be relevant and focused on the right things.

Rick Whitehead comments on the Chambers on the Profession blog post, "Internal Auditors: What Is It You Do?" (InternalAuditor.org) on LinkedIn.

Everything mentioned is true, although I would highlight two things. First, we create value. I think that the auditor should not only look for faults but also should propose improvements to add value. Second, we're guardians of trust. It's very important in our profession because if boards of directors do not trust us, our work has no purpose.

Juan Miguel Rodriguez Lopez comments on the Chambers on the Profession blog post, "Internal Auditors: What Is It You Do?" on LinkedIn.

Asian banks fear money laundering... Public-sector corruption rising... Gauging the pulse of atypical risks... Shadow IT weakens cloud security.

Update

REJECTING BAD EMPLOYERS

Workers say they won't tolerate some types of wrongdoing from potential employers.

79%	Inaction against sexual harassment
76%	Selling user data without users' knowledge
72%	Creating environmental problems
71%	Paying female or minority employees less
69%	Lobbying against consumer protection regulations

Source: The Manifest, How Do Employees Act When Faced With Unethical Company Behavior?

COMPANIES EYE INCREASED AI USE

The technology is forecast to ramp up by 2021.

Although less than 20 percent of business leaders say they currently obtain significant value from advanced artificial intelligence (AI), that number is expected to triple over the next two years, a global survey reports. Respondents say that, by 2021, the technology will increase revenue, productivity, profitability, and shareholder value for their businesses.

Competing in the Cognitive Age, conducted by Protiviti in collaboration with ESI ThoughtLab, polled 300 senior executives from companies of all sizes. Nearly one in three respondents say their organization's use of advanced AI is ahead of their competitors. Among that segment, 92 percent expect to see high value from AI as their use of the technology progresses.

Top areas in which AI is creating more value include risk management and compliance processes, cited by more than 40 percent of respondents. Forty-five percent say AI helps improve planning and decision-making, and 42 percent note accelerated time to market.

These improvements follow significant investments in AI technology. The survey found that companies each spent, on average, $36 million on AI during their last fiscal year. Respondents expect this amount to increase nearly 10 percent over the next two years.

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

IMAGES: TOP, KOVALOV ANATOLII / SHUTTERSTOCK.COM; LEFT, AGSANDREW / SHUTTERSTOCK.COM

Despite AI's many benefits, companies are facing numerous challenges in their deployment of the technology. The top five cited by participants, respectively, are uncertain return on investment, cybersecurity/data privacy, deciding on best applications, regulatory constraints, and limited AI skills/talent.

The report also notes commonalities among AI programs that address these challenges effectively. They provide decision-makers with compelling proofs of concept, for example, and well-planned pilots that can later be scaled to other parts of the organization. **— D. SALIERNO**

MONEY LAUNDERERS STRIKE FEAR

Corruption risk worries Asia Pacific banks.

After recent money laundering scandals in the region, many Asia Pacific financial institutions are concerned about continued risk of corruption. A survey by credit scoring services company FICO found that more than 90 percent of Asia Pacific banks fear they, or their peers, may inadvertently facilitate the next scandal.

Nearly two-thirds of financial-sector executive respondents from across the region cite a lack of resources as the biggest reason Asia Pacific banks remain exposed. Another 25 percent point to lack of expertise.

The survey also reveals that 40 percent of respondents assess their anti-money laundering protections as average, while 20 percent say they're unsure how they compare to industry peers. Moreover, they rate cryptocurrency, shadow banking, and property deals as the types of transactions posing the biggest threats.

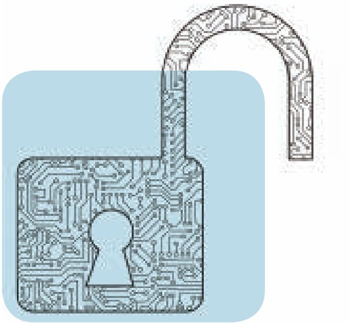
Respondents differed over the most effective way to increase money laundering compliance. Although nearly 20 percent say more severe fines and penalties is the best approach, 40 percent favor increased resources for government regulators.
— D. SALIERNO

CORRUPTION'S VICIOUS CYCLE

Public-sector wrongdoing rises in democracies such as the U.S.

Corruption is undermining democratic institutions around the world—and it's getting worse, Transparency International reports. More than two-thirds of the 180 nations and territories assessed for the organization's 2018 Corruption Perceptions Index fall below the midpoint on the scale.

Cross-referencing Transparency International's index with data from the Economist Intelligence Unit and Freedom House reveals a link between weakened democracies and rising corruption. In such nations, political leaders "have incentives to cling to power by any means, avoid prosecution, and thereby continue to enrich themselves," the report points out. In many nations, leaders have weakened laws meant to



MORE THAN
59,000
PERSONAL DATA BREACHES
have been reported to 26 national regulators since the European Union's General Data Protection Regulation (GDPR) took effect.

THE NETHERLANDS, GERMANY, AND THE U.K. HAD THE MOST REPORTED CASES, EACH WITH MORE THAN
10,000
REPORTED BREACHES.

"Sweeping data breaches under the carpet has become a high-risk strategy under GDPR," according to an analysis by U.K. law firm DLA Piper.

Source: DLA Piper, GDPR Data Breach Survey: February 2019

IMAGES: TOP, TAVARIUS / SHUTTERSTOCK.COM; RIGHT, CRAIGRJD / ISTOCK.COM

MORE VISIT InternalAuditor.org to read an extended interview with Jim Pelletier.

curb corruption, creating a vicious cycle.

"With many democratic institutions under threat across the globe," says Patricia Moreira, managing director of Transparency International, "we need to do more to strengthen checks and balances and protect citizens' rights."

While nondemocratic nations continue to suffer from public-sector corruption, cracks are showing in mature democracies, Transparency International notes. Democratic nations such as Australia and Chile have declined on the index in recent years, while this year the U.S. has fallen out of the top 20 for the first time since 2011.

Despite those setbacks, full democracies score an average of 75 on the 100-point index, more than double that of governments with autocratic tendencies and fully autocratic governments. Denmark and New Zealand top the index, while Somalia, South Sudan, and Syria are at the bottom.

In its index report, Transparency International recommends nations fight corruption by strengthening institutions and preserving checks and balances in government. It advises them to close implementation gaps between anti-corruption laws and their enforcement. Moreover, nations should empower citizens to hold governments accountable and protect press freedoms. **—T. MCCOLLUM**

ANTICIPATING SURPRISES

Emerging and atypical risks are an opportunity for internal audit, says Jim Pelletier, vice president, Standards and Professional Knowledge, at The IIA.

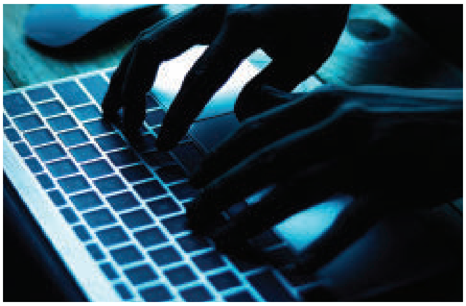
The 2019 North American Pulse of Internal Audit study notes internal audit's ability to identify atypical risks isn't keeping pace with the frequency of surprise risks reported by management. How can internal audit help assess these risks? Boards most commonly turn to executive management for information on emerging and atypical risks, but it's a serious governance concern if they aren't searching for input from others, particularly their chief audit executive (CAE). This represents a clear opportunity for internal audit to position itself as *the* objective source of information on emerging and atypical risks.

CAEs need to carve out enough time to strategize no matter the size of their department. They need to challenge their own risk assessment practices. Are they simply a mirror for what management is willing to share, or are they providing insights beyond that feedback? They should develop a data strategy and start planning for the resources they'll need to execute it. Most importantly, they need to be effective with their limited time with the audit committee and board. This involves understanding their audience and needs; being prepared to deliver meaningful, objective information; and speaking out on difficult issues.

Download the 2019 North American Pulse of Internal Audit at http://bit.ly/pulse2019.

OUT OF THE SHADOWS

Employees are weakening cloud security.



Shadow IT—employees' use of unsanctioned personal devices, cloud services, and apps—is undermining organizations' cloud security and putting data at risk, according to the Oracle and KPMG Cloud Threat Report 2019. Ninety-three percent of respondents are dealing with rogue cloud app usage, notes the survey of 450 cybersecurity and IT professionals from Asia, North America, and Western Europe. Half cited lack of security controls and misconfigurations as reasons for fraud and data breaches.

Kyle York, vice president of product strategy at Oracle Cloud Infrastructure, says there's a heightened need for a coordinated, integrated, and layered security strategy because "the world's most important workloads are moving to the cloud." The report projects that the number of organizations with more than half their data in the cloud will more than triple by 2020. Most of this cloud data is sensitive, 71 percent say.

Other areas presenting security challenges include confusion about chief information security officers' role in securing software as a service, and detecting security incidents in the cloud. **—S. STEFFEE**

PHOTO: LEFT, JARIRIYAWAT / SHUTTERSTOCK.COM

Back to Basics

BY ANDREW TOPA EDITED BY JAMES ROTH + WADE CASSELS

DISSENT IN RISK MANAGEMENT

Employees' perceptions about conveying disagreement can influence the way they respond to assigned duties.

Employee communication of dissent, or constructive challenges, to management and its corresponding reception, are key aspects of risk management. Employee perception about conveying disagreement influences that employee's understanding of controls, and his or her conscious or unconscious willingness to execute assigned duties.

Implementing a risk response—deadlines, checklists, reviews, and other specified assignments—may not coincide with the desires of the process owner tasked with completing them. This disconnect between the goal of management and the desires of the process owner is a prime source of dissent, which, in turn, affects the success of the risk response.

Specific steps precede an employee's decision to express dissent. First is the awareness of the issue, followed by the attribution of personal responsibility for responding, and then the estimation of the response. The decision to express dissent then involves weighing the possible change against the anticipated backlash.

There are typically three types of dissent: articulated, antagonistic, and displaced. Because internal auditors must include an assessment of communication channels when testing the design and effectiveness of controls, it is important that they understand the role that dissent plays in a risk management program and how dissent can influence control effectiveness. By doing so, auditors can identify sources of control failure not immediately recognizable when the control is evaluated in isolation.

Articulated Dissent

Articulated dissent is the direct communication of dissent by employees to individuals with the authority to influence organizational change. Employees choose this method because they believe the dissent will be received positively and seen as constructive feedback. Articulated dissent is influenced by a perception that retaliation will be minimal and a conversation with management is positive. Employees will use articulated dissent when it is perceived that the organization is accepting of criticism. It involves an active effort to change the organization for the better from within.

Antagonistic Dissent

Antagonistic dissent is used by employees who believe that dissent will be received as adversarial, but that the feedback they provide will ultimately be safeguarded against retaliation. This strategy is used by employees in roles that provide a sense of organizational leverage—based on position, expertise, or relationship—and the perception of immunity against reprisal. Antagonistic dissent is primarily used to oppose issues that have a personal connection to the dissenter. Employees express dissent to

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

audiences that are captive or influential, and it occurs in low retaliation conditions. The dissent is intended to change the organization from within, but primarily in a direction that is most beneficial to the individual. Although the underlying motivation for dissent can be self-oriented, the change may be a positive for the organization.

Displaced Dissent

Displaced dissent is used when the employee believes that feedback will be perceived as adversarial and will lead to some form of retaliation. This dissent is communicated to an audience that is either outside of the organization, inside of the organization but lacking any authority, or composed of employees at a similar level. External audiences include spouses, non-work friends, or family members. Internal audiences include fellow co-workers who lack the ability or authority to address the concern. These audiences are chosen because of the low risk for retaliation and for the sense of community that comes from shared displeasure. Displaced dissent involves expressing disagreement without confronting management directly. It is a common predictor of employee exit because employees internalize their disagreements without communicating them to those with the power to help. The physical exit of the employee is preceded by a psychological exit—the employee "checks out" and loses his or her commitment to the organization.

Understanding Dissent Strategies

An effective risk management program must consider the dissent strategies used by employees. How employees choose to express their constructive challenges can have a material impact on a risk management strategy. When a control is designed using a risk-based approach, the design process often omits an understanding of how the employee tasked with implementing it will receive the instructions.

Because risk responses are performed by front-line employees, dissent that is unknown or unseen by management affects the efficacy of the strategy. When employees engage in a displaced or antagonistic dissent, their interpretation may differ from that of management; they may view the internal controls to which they are assigned as restraints on their ability to work effectively. If this perception is coupled with a lack of effective communication channels, the employee is left with dissent options that are disadvantageous to the organization (antagonistic or displaced dissent). This dissent action can result in key controls failure because the employee feels unable to express concerns about the control, itself, or its impact on other job functions.

Internal control failure may be misinterpreted as a failure in design when the breakdown stems from a lack of avenues for employees to express dissent. Employees who believe they have no reasonable means of communication with management redirect their dissent toward their assigned duties, resulting in a negative impact on the organization.

Managing Dissent

To mitigate the negative effects of dissent on risk management, management should evaluate communication channels available to employees. Does the organization provide reasonable outlets for employees to communicate disagreements and disputes? Do these outlets provide the support and confidence to empower employees? Communication channels are the formal and informal mechanisms in place for capturing and addressing employee concerns.

Organizations with a focus on governance, risk, and control are likely to have the formal aspect covered, whether through third-party hotlines, official human resources policies, regularly scheduled one-on-one meetings, or a combination thereof. What is missing is a recognition of how organizational culture influences their use and effectiveness. When the culture set by management through formal and informal policies includes an openness toward opposing viewpoints, employees then view the reception of dissent as positive and are more likely to express it in ways beneficial to the organization.

Managers and stakeholders should recognize their organization's culture in strategic decision-making. A better understanding of the culture can come from surveys of employee attitudes, a formal audit of information flow between organizational levels, or other assessments of communicative effectiveness.

Appropriate communication channels for the expression of dissent must be supplemented by training for managers on the types of dissent and how each should be addressed. Additionally, strong organizational policies should formalize the organization's attitude toward dissent. These policies should provide clear direction to managers and employees on how the organization approaches the expression of dissent and specific procedures for the expression and management of these opinions.

Communication Is Crucial

It is important for employees, managers, and auditors to understand the communication channels employees use to express dissent, and how each of these may affect the organization's strategic goals. Ultimately, the role of dissent in employee attitudes and behaviors is a key component in determining if a risk management program can succeed. Ia

ANDREW TOPA, CRCM, *is manager, compliance audit, at TF Holdings in Fort Worth, Texas.*

Advertisement

Case Study: ArcelorMittal

Integrated Assurance: One company's journey to topline integrated assurance maturity

The world's leading steel and mining company reaches unprecedented levels of efficiency with the help of an Integrated Assurance platform for its corporate audit function.

ArcelorMittal

In 2016, ArcelorMittal merged its Internal Audit (IA) and Sarbanes-Oxley (SOX) functions under Global Assurance, which also comprises the Enterprise Risk Management and Group Security functions. This assurance model follows the governance and monitoring of three lines of defense under a single umbrella, delivering on a mandate to align people, processes, tools and methodologies — and gain synergies.

> "We are happy to have positioned ArcelorMittal amongst the leading practices in Governance, Risk and Controls, having integrated our Internal Audit and SOX functions into the new Integrated Assurance platform."
>
> **- Francis Lefèvre**
> Chief Audit Executive and
> Head of Global Assurance

By 2018, ArcelorMittal had already achieved topline maturity on the Integrated Assurance Maturity Curve developed by Richard Anderson from DePaul University and Wolters Kluwer. The company had also realized a reduction in audit fatigue, marked the removal of duplicate testing, and benefited from overall efficiency gains.

"We are happy to have positioned ArcelorMittal amongst the leading practices in Governance, Risk and Controls, having integrated our Internal Audit and SOX functions into the new Integrated Assurance platform," says Francis Lefèvre, Chief Audit Executive and Head of Global Assurance. "This integration is well aligned with all our other digitalization and automation initiatives undertaken in Global Assurance to gain efficiencies and enhance our audit coverage while maintaining our quality standards."

The magnitude of these gains in efficiency stands out against the backdrop of the company's former assurance activities. Viji Ganesan, IT Manager, Competence Center and architect of the Integrated Assurance project, puts the learning curve in context.

"When we merged Internal Audit and SOX into Global Assurance, each was working at a different level of technology expertise," she says. "We needed to get them speaking the same language. Our Internal Audit team was already using an audit management system. That system was developing a next-gen product that added the functionality of a content management offering. We believed the new product could get all teams working on the same assurance platform. So we decided to leverage our existing investment: We set to work standardizing IA and SOX within a single platform."

Wolters Kluwer
When you have to be right

Integrated Assurance delivers reporting transparency and meaningful insights.

Ganesan doesn't have to think twice about the product's most valuable benefit for the geographically organized Global Assurance function.

"The reporting potential is incredibly powerful," she says. "We now have the ability to report on secondary dimensions or reporting structures common to both audit and SOX. This option opens up so many unexplored opportunities for us. The common reporting platform for IA and SOX is a brilliant place from which to launch any other digitalization project we might wish to undertake."

As anticipated, the tool's historical insights capabilities quickly proved an indispensable benefit to Global Assurance as well. "Now we can see if a control has already been tested in SOX control assessments or in an audit project," explains Ganesan. "All the historical issues at entity level are right there."

Head of Competence Center Andreas Trogsch has been just as pleased with the outcomes to date. "I'm particularly proud of how the Competence Center piloted the product in its early stages," he says. "We engaged with our various critical stakeholders. We influenced the decision of early adoption. And we led the Integrated Assurance implementation, blending expertise of technology and methodology in close collaboration with our product vendor."

> "We now have the ability to report on secondary dimensions or reporting structures common to both audit and SOX."
>
> **- Viji Ganesan**
> IT Manager,
> Competence Center

Standardization starts with a common taxonomy.

ArcelorMittal has a huge geographic footprint for a corporate audit function. Global Assurance consists of more than 200 personnel placed in over 25 countries across the Americas, Europe, Africa/Asia/CIS and Mining regions. Global Assurance alone had hundreds of SOX risk control matrices (RCMs) of varied sizes and shapes.

When the function kicked off the Integrated Assurance project, Internal Audit were already advanced users of their audit management system. However, SOX teams had been operating exclusively for many years using Excel spreadsheets for their RCMs.

To resolve the disparity in technology, the Global Assurance Competence Center called on external consultants to standardize the SOX RCM, along with SOX common control objectives across business cycles. They also harmonized terminology across IA and SOX within the context of live pilots run on mature regional teams from the U.S., Canada, South Africa, Luxembourg, Romania and Mining.

"A key project objective was to standardize Internal Audit and SOX methodologies into one common methodology," says Brian Watts, Manager, Competence Center. "That effort helped us decrease audit fatigue, reduce duplicate testing, create a single RCM, and perform integrated reporting."

Successful pilots pave the path for stakeholder buy-in.

As the starting point for the standardization process, the live pilots created the framework needed to build a uniform data model from common terms of reference between IA and SOX. "These pilots had representation from SOX experts and audit heads," says Ganesan. "They gave us our first taste of user experience feedback."

Ganesan and her team wrapped the pilot phase having tested two versions of the tool. They also performed a gap analysis of the technical and functional points they wanted to cover, and arrived at a minimum viable product for installation.

"We were able to show the audit managers how this single tool could help standardize Internal Audit and SOX," she says. "We knew we'd gain historical insights at an entity and control level. And that this context would give visibility of SOX work to Internal Audit (and vice versa). In other words, no more duplicate testing."

A highly structured training program supports change management.

"It was a perfectly packaged program," says Ganesan. "Everybody got on board, because they had the support and resources they needed to fully understand the changes."

- **Viji Ganesan**
IT Manager,
Competence Center

ArcelorMittal management understood the Integrated Assurance platform had already opened new avenues for productivity tracking, combined issue reporting, and joint IA and SOX risk assessments. They recognized as well the potential of powerful reporting structures, extensive audit trails, increased accountability and a common database taxonomy between IA and SOX.

Yet they also understood that no matter how revolutionary a new tool or process, change management is where rubber meets pavement with of a project of this scale. So Ganesan and her team took a very disciplined approach. "We spent about a month just designing the user guides with the help of our vendor," she says. "Everything was tailor made for us."

These comprehensive user guides detailed the complete audit and SOX lifecycles. The team also produced a series of 5-minute training videos to cover every aspect of these lifecycles. Finally, they taught classroom-style webinars to 15 groups around the globe.

"It was a perfectly packaged program," says Ganesan. "Everybody got on board, because they had the support and resources they needed to fully understand the changes."

Collaboration calms migration complexity.

Jumping in on the ground floor of the platform's development opened up a world of unknowns for the Global Assurance function. For one thing, there was no data migration path to take them from the old audit tool to its next-gen counterpart. However, Lefèvre believed in the tool's potential, and ultimately deemed it a risk worth taking. Knowing Global Assurance would face many challenges as early-bird adopters of the tool, Lefèvre asked the Competence Center to implement the tool jointly with audit teams.

ArcelorMittal worked closely with consultants from their vendor to build migration aids. And in the end, the team migrated thousands of historic recommendations to the new tool, addressing showstopper risks as needed. Along the way, they took advantage of the tool's advanced features, assigning secondary dimensions to 3 years' worth of old issues for optimal reporting.

Secondary dimensions and stakeholder engagement address reporting differences.

Not every organization has the willingness or the support to take such bold steps toward reducing complexity. But their early successes with the classic tool gave ArcelorMittal the confidence to use it creatively. They wasted no time turning the tool's capabilities on the company's SOX landscape, which happens to be dependent on legal entities.

"SOX reports at a deeper level of the organization hierarchy than Internal Audit," Ganesan explains. "But we've taken full advantage of the tool's flexibility to address the challenge. We kept the hierarchy used by Internal Audit, adding legal entities as secondary dimensions. We did something similar for joint risk assessments."

As SOX started working in the new tool, they faced challenges that included shared controls testing, IT controls testing and reporting requirements for external stakeholders. But they rose to the challenge with successful steps that included holding workshops and collaborating with vendors in small working groups.

"The implementation of common tool for audit and SOX work is a key element in supporting the integrated methodology of Global Assurance at ArcelorMittal," says Christian Quincke, Regional Manager, Europe, and Global SOX Coordinator.

"Our challenge here is twofold: We must develop solutions that fit the quite business and organizational models in the group. We must also ensure common standards to facilitate local and group-level reporting and knowledge sharing. Today, we're well placed to leverage these benefits, even as we continue to develop the tool to get more integration between SOX and audit work."

"I'm particularly proud of how the Competence Center piloted the product in its early stages. We engaged with our various critical stakeholders. We influenced the decision of early adoption. And we led the integrated Assurance implementation, blending expertise of technology and methodology in close collaboration with our product vendor."

- Andreas Trogsch
Head of Competence Center

Innovation transforms the external audit process for SOX Team USA.

In an interesting plot twist, certain regional differences have inspired important innovations in the context of Integrated Assurance — most notably in the United States. Due in part to its organizational structure, the Global Assurance U.S. team led by Wael Shannak has historically found ways to prioritize transparency in their SOX reporting with external auditors.

But with the help of the tool, they've pioneered an altogether different kind of visibility, says Ganesan. As they imported the SOX RCMs and started testing, the U.S. team, onboarded 20 external auditors into the tool, training them to use the Integrated Assurance platform.

"The U.S. team has benchmarked itself on transparency," says Ganesan. "Now, external SOX auditors get access to all SOX work in real time. That includes everything: work completed, work in progress, all work papers, all issues raised. This is real innovation, and a clear win-win situation."

Neelakantan Venkatachalam, Regional Manager for the Americas, sees the promise of many more wins down the line.

"The Integrated Assurance project is a critical element of the overall digital transformation being implemented in Global Assurance," he says. "It's an excellent example of client/consultant collaboration. Together, we've developed a world-class product that covers both Audit and SOX, and provides transparency, scalability and security. We expect to benefit from more efficiencies as the implementation cycle matures and the application gets fully integrated within our digital strategy."

Enterprise-wide participation creates game-changing opportunities.

Regional SOX transparency isn't the only innovation the tool has helped facilitate. As part of the risk assessment process, each country head now has the possibility to look at strategic risks on the Integrated Assurance platform. They can enter IA, SOX and forensic risks for their own country. They can also view imported strategic risks from the platform of the Global Assurance Enterprise Risk Management (ERM) team.

With each country adding important pieces to the puzzle, Global Assurance has built a comprehensive registry of more than 2,500 risks in a single assessment. This registry provides a complete heatmap, with drill-down possibilities that include risks tied to entities and rated by impact and likelihood.

The team also realized early on they could report across their entities on risks. "Today, we're able to quantify our controls and analyze which are manual and which are automated," says Ganesan. "Going forward, we can look at optimizing projects even further."

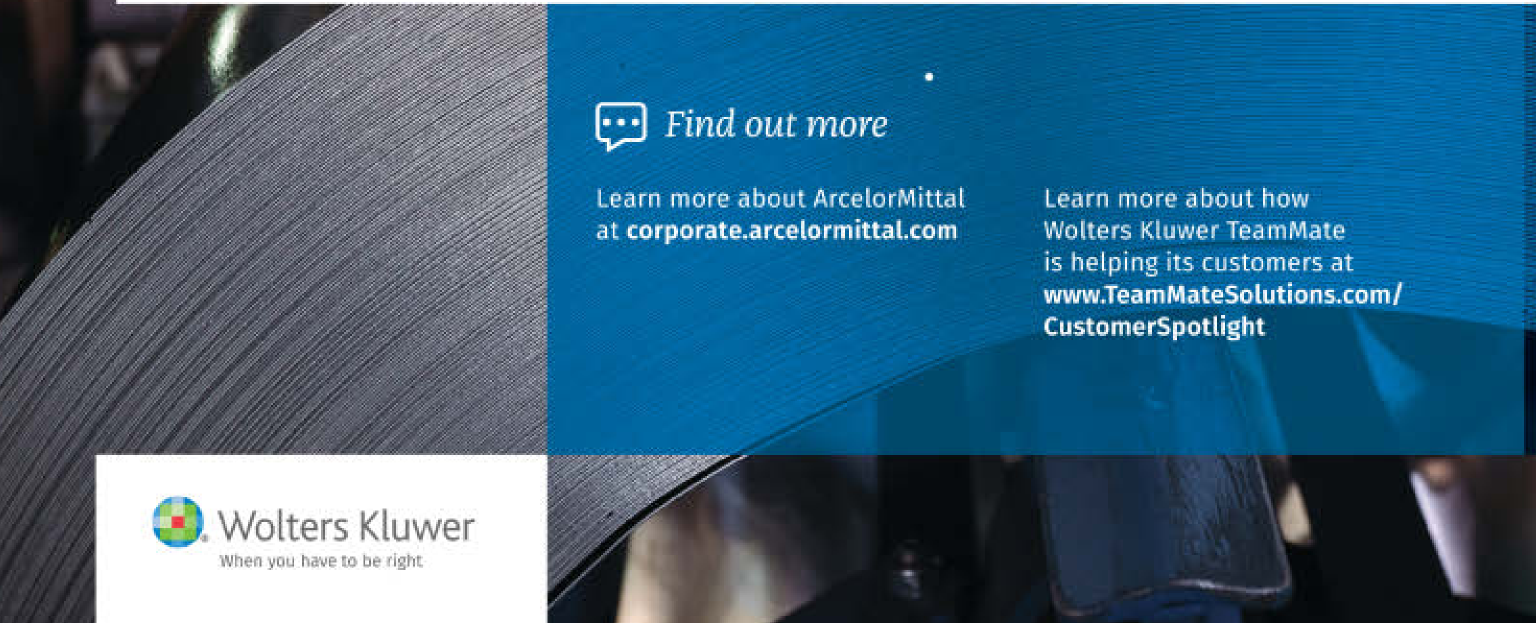
Regional Manager of Mining and Corporate Audits Kuntal RoyChowdhury shares the same optimism. "This tool," he says, "could be one of the key elements to enhancing the overall efficiency of the assurance function by reducing duplication, incorporating all audit and compliance work into one reporting platform, and providing a single view to stakeholders."

The future of Integrated Assurance starts with a bold vision.

"Organizations of the future increasingly exhibit digital characteristics in various shades and intensity," says Vishal Arora, Regional Manager, AACIS and GA Digitalization Co-ordination. "We have a massive wave of digitalization happening across the organization. As part of its vision and mission, Global Assurance alone has several automation and analytics projects in progress. To date, we're happy with what the platform offers, helping us achieve top line maturity on that Integrated Assurance maturity model."

Never content to rest on today's wins, Global Assurance has big plans for where to take ArcelorMittal with the support of the Integrated Assurance tool. According to Ganesan, this vision includes building Bots on top of the tool for quality assurance and improved efficiency with automation of repeatable tasks. It also includes continuing to push the boundaries for close collaboration with its business contacts, auditees and control owners.

With the help of the platform, the group is moving toward Control Self-Assessments and Risk Self-Assessments — and publishing audit reports to external auditors. "This tool has been our great enabler," says Ganesan. "We're just getting started."



Find out more

Learn more about ArcelorMittal at **corporate.arcelormittal.com**

Learn more about how Wolters Kluwer TeamMate is helping its customers at **www.TeamMateSolutions.com/CustomerSpotlight**

Wolters Kluwer
When you have to be right

ITAudit

BY STEVE MAR

THE SINGLE POINT OF FAILURE

The death of a CEO highlights the risks of only one person controlling access to corporate data.

When Canadian cryptocurrency exchange CEO Gerald Cotten died unexpectedly in December, he took key corporate passwords to his grave. Those passwords could unlock $137 million in customer funds that were trapped on Cotten's encrypted notebook computer. Without the recovery key to access those funds, his company, QuadrigaCX, filed for bankruptcy, according to Nova Scotia's Supreme Court records.

In March, court-appointed monitor Ernst & Young (EY) cracked Cotten's code and found the funds had been transferred out of customers' crypto wallets in April 2018. Moreover, EY says QuadrigaCX kept limited records and never reported its financials.

This incident takes the meaning of a single point of failure to a higher level. It also suggests some considerations for internal auditors now and in the future.

At QuadrigaCX, basic governance, risk management, and controls failed to prevent this unexpected and disastrous event or allow for a timely recovery. Clearly, access controls stopped the company from running the key cryptocurrency exchange process and transacting with its customers normally.

All organizations need to think about single-point-of-failure risks such as one person knowing all the key passwords to a critical process. This risk occurs when failure of one part of a system stops the entire system from working. This condition is undesirable in any system with a goal of high availability or reliability . This is what happened at QuadrigaCX, which raises important questions and lessons in three key areas.

Technology Governance, Risks, and Controls

Internal auditors should identify critical business technology governance, risks, processes, and systems to determine whether single points of failure exist. IIA Standard 1210.A3: Proficiency calls on auditors to know the business and technology they review, which they can accomplish by learning, documenting, and mapping key processes and systems. As part of that process, the auditor may analyze the process flow and identify whether certain devices or processes could become a single point of failure. For example, in some network configurations, a single router or device may serve as a key gateway. But if the one device fails, the gateway may become unavailable to users.

Likewise, a single software failure can have a calamitous impact on a business. In 2012, a failed software test at Knight Capital caused the company's new trading system to start trading repeatedly, resulting in a $440 million loss within 45 minutes.

Information security tools or systems can become

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

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

a single point of failure, too. For example, a retail company requested that all of its customers update their sign-on passwords, telling them it would give them promotional discounts and improve account security. However, the password security system became a single point of failure when suddenly too many customers logged on to update their passwords, which crashed the system. The system was not designed to handle the volume.

In addressing single points of failure, internal auditors should focus on the highest business process and technology risks. For example, Deloitte's An Eye on the Future 2019: Hot Topics for IT Internal Audit in Financial Services report lists cybersecurity, technology transformation and change, technology resilience, and extended enterprise risks among its hot risk topics. Several of these topics apply to all organizations.

Knowing the top risks represents a start, but finding single points of failure in those areas can be challenging. Internal auditors cover program changes by testing governance and controls, but at best, auditors can only sample certain testing procedures and processes.

Disaster Recovery Backup Testing

Internal auditors should determine what recovery or backup plans are in place for the organization's critical systems. Disaster recovery plans serve as a high-level control process to restore critical systems that were lost or disrupted. Reviewing the governance, risks, and controls over backup or disaster recovery tests allows the auditor to determine how rapidly a critical system can be recovered. The objective of recovery testing should include looking at any single points of failure such as testing for missing documents, devices, or key individuals.

Use of cloud technology and software as a service adds different factors that the auditor needs to review. For example, how frequent and how realistic are the testing plans? What mistakes or setbacks are uncovered, and more importantly, are there any single points of failure? If a critical system recovery was performed but needed a single person to provide the only passwords to transact or start the system, then the auditor or recovery team should consider this a single point of failure.

Some technology recovery plans are not completely tested or exercised because they are too complex, no resources are budgeted, or the governance is too weak. Sometimes limited recovery is considered successful.

Several years ago, during a large payroll processor's data center disaster recovery test, an IT audit team observed that a critical system failed to restore several times. The culprit: One backup medium failed and could not be read. The disaster recovery team was able to get a new backup made but from the existing data center. This backup took more than two days to create. What would have happened if the existing data center had been unavailable or if it took weeks to restore? Would the payroll processor's customers accept this critical service disruption?

Key Personnel

Auditors should look for key personnel or executives as a single point of failure in their audit universe or audit program. If a privileged account user, system administrator, or CEO is the person who knows the key password, and no other person or recovery process is in place, then the risk of a single point of failure increases.

> Auditors should look for key personnel or executives as a single point of failure in their audit universe.

To begin, internal auditors should identify who the key stakeholders—customers, vendors, or users—are for the critical systems. They should inquire and document whether any single individual performs a critical task or function and consider the single-point-of-failure risk.

Key personnel do not need to be a CEO to become a single point of failure. During a review of a large retailer's critical key management system, an IT auditor discovered that one of the two individuals who had half of the primary encryption key had left the company. The company noticed this situation because it had not needed to generate a new key since the employee departed. If it had needed to generate a new key, a serious delay or security incident may have occurred.

Prepare for the Future

Preparing for the future, internal auditors need to continue assessing complex IT processes based on risk. The QuadrigaCX incident demonstrates that auditors need to assess possible technology single points of failure. When a single point of failure can disrupt an organization's business or technology process, auditors need to carefully assess this threat. Ignoring it could be hazardous to the organization's health. Ia

STEVE MAR, CFSA, CISA, *is an instructor of IT audit at Seattle University and the University of Hawaii in Honolulu.*

THE IIA WOULD LIKE TO THANK OUR SPONSORS FOR HELPING MAKE GAM 2019 A SUCCESS!

Silver Sponsors

AUDITBOARD

EY
Building a better
working world

Grant Thornton

KPMG

protiviti®
Face the Future with Confidence

The Financial and
Risk business of
Thomson Reuters
is now Refinitiv.

REFINITIV™

Bronze Sponsors

acl™

pwc

RSM

2019-2310

GAM
WHERE LEADERS EVOLVE.

#IIAGAM

IIA®

BY SRIDHAR RAMAMOORTI, JAMES H. WANSERSKI + RICHARD STOVER EDITED BY CHARLIE WRIGHT

THE VELOCITY OF RISK

In a time of instant crises, internal auditors and their stakeholders need a sense of urgency to identify and manage risk.

Only a few decades ago, the onset of problematic risk events often was slow, and organizations handled the corresponding aftermath over a manageable time frame. Organizations armed with extensive public relations resources responded to most post-event crises after planning and analyzing thoughtful responses. Additionally, organizations carefully calculated their transparency with stakeholders regarding the event to manage its impact on the organization.

Fast forward to today, and the pace of information is almost instantaneous. For example, when a popular U.S. fast food restaurant chain experienced an outbreak of E. coli-infected lettuce, its stock price decreased 44 percent within 90 days amid intensive social media and news exposure. Recent privacy concerns directed at various social media companies caused stock valuations to drop within minutes and led to immediate calls for government investigations. Disclosure of inappropriate sales arrangements by a large U.S. financial institution caused a significant upheaval, including important personnel changes.

In today's environment, the timing between a catastrophic risk-driven crisis and the financial and reputational decline for an organization can be practically simultaneous. This new reality has forced senior executives and internal auditors to consider a new aspect of risk management—the velocity of risk.

The velocity of risk is the speed or ferocity with which events occur in today's business environment. Auditing within this "new normal" means changing, adapting, and understanding the imperative to respond to the speed of change with a strong sense of urgency. Supplemented by awareness of the velocity of risk, internal auditors can identify and address areas where organizations must take preemptive actions to reduce the possibility of a crisis caused by a catastrophic risk event.

Velocity and ERM

The *International Standards for the Professional Practice of Internal Auditing* frames the execution, conduct, principles, and practices that also serve as "guardrails" for the profession. The standards relevant to the velocity of risk logically connect with internal audit competencies such as demonstrating competence and due professional care; aligning with the organization's strategies, objectives, and risks; providing risk-based assurance; being insightful, proactive, and future-focused; and promoting organizational improvement.

Internal auditors contribute in myriad ways to enterprise risk management (ERM) goals by:

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

TO COMMENT on this article, EMAIL the authors at sridhar.ramamoorti@theiia.org

- Helping management manage risk.
- Assessing and auditing risk assessment methods and approaches.
- Creating a responsive, nimble, and agile audit plan.
- Evaluating whether ERM programs are using the right metrics.
- Assessing whether management is prioritizing risk appropriately.
- Supporting and educating the board and senior management on recent advances in risk management thinking.

Often, internal audit will review how the organization is addressing the chief risk officer's enterprisewide risk assessment, providing assurance about the prioritization and adequacy of response strategies. These assessments will include internal audit's perspective of all the organization's operations directed toward risk considerations. That perspective should include risk areas that potentially are detrimental to the organization, as anticipated by assessments of probability, size, and speed of impact. Internal audit should target the corresponding areas within the scope of its work program.

In performing these duties, internal auditors should ensure the organization's ERM program matrix highlights how velocity of risk can impact the organization. Auditors should recommend making it one of the risk program's key metrics.

Auditing the velocity of risk can ensure risks are more appropriately prioritized and management is able to more effectively prevent, manage, and respond to risks. Internal auditors can help management and the board measure and address catastrophic risk by understanding the specific risks that could impact the business, measuring risk in an organized and systematic way, and documenting and communicating those quantitatively and qualitatively assessed risk perspectives.

Planning and Execution

Internal auditors must consider the velocity of risk when prioritizing and creating their annual audit plans. The audit plan should include a risk velocity measure that reflects the magnitude and speed of reaction internally and externally should a catastrophic risk event occur. The department should adjust its perspective on risk management by recognizing and addressing velocity's influence on likely events and impacts. Internal auditors must be aware of risk's current and ongoing impacts on the business in designing and executing audits, compiling results, documenting historical trends, and communicating how management, business processes, and embedded technology are addressing risk. Moreover, auditors should assist and influence management teams to better calibrate, anticipate needs, and frame the impact of velocity on risk-event preventive actions.

In performing their work, internal auditors must become familiar with the phrase "auditing at the speed of risk." Post-catastrophic risk event reactions tend to be much costlier and more detrimental to an organization. Auditors should anticipate risk-related events by using continuous monitoring tools and auditing through the systems via queries, specialized exception reporting, and similar techniques. These methods teamed with including "velocity of risk" as a parameter in risk-matrix discussions can highlight at-risk business processes and transactions, increase coverage, and add speed. For example, internal auditors can equip themselves with tools and techniques such as trended historical transaction reviews within supply chain operations.

These methods—supplemented by vendor-by-vendor analytics, internal control reviews, and interviewing techniques—can lead to earlier detection of fraudulent transactions, timing discrepancies, wasteful or nonoptimal spending, and product defects. Integrating velocity of risk into internal audit's environment, along with a sense of urgency, can add to overall effectiveness, improve organizational agility and resilience, and contribute value to management.

The Third Dimension of Risk

The velocity of risk is pushing the internal audit profession to grow and support its own and management's awareness of risk's speed of impact by accelerating and enhancing risk-based auditing. Connectedness to business risks and strategies now is even more imperative for internal audit to maintain its relevance. To keep pace, businesses need to embrace a three-dimensional risk management approach: probability, impact size, but most importantly, velocity—that sense of timing, speed, and mean-time-to-event mentality.

By adding the dimension of velocity, internal audit can facilitate deep-dive assessments of certain risk areas that could become catastrophic risk events. Identifying these areas can inspire a more robust dialogue with management and the board about how to remedy potential issues. Moreover, addressing the velocity of risk can enable internal audit to help management and the board anticipate and prevent these crisis events from occurring. Ia

SRIDHAR RAMAMOORTI, PHD, CIA, CRMA, CFSA, *is an associate professor of accounting at the University of Dayton in Ohio.*

JAMES H. WANSERSKI *is founder of Wanserski & Associates in Atlanta.*

RICHARD STOVER, CPA, CGMA, *is a lecturer at the University of Dayton.*

BY ANNA HOWARD + ANDREW LOUGH EDITED BY BRYANT RICHARDS

THE SOCIAL ENGINEERING FRAUD

National culture plays a part in a whaling fraud that snares the controller at an overseas subsidiary.

Kai Tang was working late on Dec. 25. It was year-end, so activity in the company was picking up, keeping the controller of the thriving Singapore distributor of a large U.S. manufacturer busy. Because it was a holiday in the U.S., Tang knew he would not be interrupted by inquiries and requests from corporate headquarters. Although the corporate controller and the chief financial officer (CFO) rarely visited him in person, they frequently emailed him with questions, but only called on urgent matters due to the time difference. Additionally, his subsidiary was visited by internal auditors the month before—which didn't raise issues—and they were due for a visit from external auditors in January.

Tang suddenly received an email from the company CEO notifying him of a building purchase for a new office location in Asia. The email expressed urgency in wiring money to close the deal. Tang rarely communicated with the CEO directly, but he knew he had a bad temper and did not tolerate being questioned or challenged.

As Tang contemplated how to contact his general manager—who was on a plane—and how and whether to reach the company's CFO at home on Christmas, his phone rang. The man introduced himself as a senior manager at the company's external audit firm. He stated that he was working with the CEO on this urgent purchase and that Tang's delay of the wire would jeopardize the whole deal. Though his head was spinning, and he had lingering questions, Tang hurriedly prepared the $100,000 wire, confirmed the account information, and clicked "send." This turned out to be a scam and the funds were never recovered by the company.

The next month in the boardroom, as the multinational company tried to understand how it became the victim of such a trite, albeit somewhat sophisticated, scam, board members asked, "What questions did we not ask that could have prevented this?" Several reasons were named in creating this perfect storm of a failure, including national culture, which was brought up more than once.

Dutch social psychologist Geert Hofstede found that six cultural dimensions are at play in the global marketplace. One of them is the Power Distance Index (PDI) that measures the distribution of power—and wealth—between individuals in a business, culture, or nation. In a country like Singapore, where a stronger hierarchy of authority exists, it is common for subordinates to follow the whims of an authoritative figure. As a general rule, in higher PDI cultures, subordinates

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

TO COMMENT on this article, EMAIL the authors at anna.howard@theiia.org

LESSONS LEARNED

- » Following the letter of the control description is not enough. Ask questions regardless of whether the goal of the control is accomplished and revise the description, if necessary.
- » Company management should work with outside vendors, such as banks, to automate controls.
- » Employee training should be conducted by management or expert consultants to recognize and identify phishing schemes. The training should be comprehensive and frequent.
- » When working in a multinational environment, learn about national culture, identify traits that might facilitate fraud, design more robust controls, if needed, and provide additional coaching to employees.
- » Management should create a support structure and invest time to establish personal relationships with foreign employees to cultivate trust.

are less likely to question their superiors than in low PDI cultures and organizations where authority figures work more closely with subordinates and it is more acceptable to challenge authority.

Dessalegn Getie Mihret of Deakin University in Australia conducted a study of 66 countries testing the association between national culture dimensions and exposure to fraud. His research suggests high fraud risk exposure in countries with high PDI. This was a case of external fraud but a fraud, nonetheless. In Tang's case, this cultural dimension had a double effect. Tang, being from Singapore, a high PDI culture, was uncomfortable challenging the request of the person he perceived to be the high authority. The CEO of the company was from Albania, another high PDI culture, and was infamous for not tolerating any challenge to his authority. This created a culture of fear within the company. Nobody wanted to be reprimanded by the CEO, who was known to yell and belittle his employees in public.

The controls proved to be poorly designed for any kind of culture.

Another factor in this perfect storm of breakdowns was the absence of trusted advisors within the company with whom Tang could consult in the time of doubt. Because it was a holiday, Tang did not feel comfortable contacting any of his supervisors in the U.S. He did not have a close enough relationship with any of them and felt he'd be bothering them. Trust is paramount in relationships, especially in Asia, and it takes an investment of time to build it. None of the U.S. managers invested time in creating close connections with their Singaporean colleagues.

Whaling is a type of attack that uses email or website spoofing to trick the target into performing a specific action, which in this case was having the controller transfer money to an account. Cybercriminals pose as senior players within an organization targeting other important individuals at the organization with the goal of stealing money or sensitive information, or gaining access to the computer systems. Specifically, whaling targets key people with what appears to be communication from someone senior or influential—such as the CEO—with a request that staff are reluctant to refuse.

Internal controls help prevent such things from happening, but the existing system proved ineffective in overcoming such a strong cultural influence. In fact, the controls proved to be poorly designed for any kind of culture. The only control over bank wires was written as:

> *Wire transfers are submitted on the bank website. For wire payments, all the backup is given to an authorized signer, the controller/general manager/finance manager for electronic approval on the bank website.*

Every time this control was tested during an internal audit, the controller was able to produce the documents of the secondary approval by the general manager. The letter of the control was followed. The internal auditors never asked, "Would it be theoretically possible for one person to approve and send the wire on the banking website?" Evidently, the bank website did not require a secondary approval, which allowed one person to send the wire out.

Additionally, there was a breakdown in IT security controls. The email was clear evidence of a successful phishing scheme where an attacker posed as a reputable person with the intent to defraud the organization. Adequate training to educate employees is critical to prevent these attacks and was obviously lacking in Tang's case. Ia

ANNA HOWARD, CPA, CMA, *is director, Master of Science in Accounting Program, at Nichols College in Dudley, Mass.*

ANDREW LOUGH, CIA, CPA, CRMA, CGMA, *is an adjunct professor of internal control audit at Nichols College.*

GDPR's Global

If U.S. businesses believed the broad waters of the Atlantic would save them from the European Union's new General Data Protection Regulation (GDPR), that illusion was dispelled on Jan. 21. That was the day on which the French privacy regulator Commission Nationale de l'informatique et des Libertés (CNIL) fined Google about €50 million ($57 million) "for lack of transparency, inadequate information, and lack of valid consent regarding the [sic] ads personalization."

NOYB–European Center for Digital Rights and La Quadrature du Net—two privacy activist groups—brought

Reach

Internal auditors around the world are starting to learn the impact of Europe's data protection regulation on their organizations and their role in compliance.

Arthur Piper

Illustration by Sean Yates
Base photograph by Viktorus/Shutterstock.com

the case almost as soon as GDPR came into effect on May 25, 2018. They claimed that users could not give specific consent for Google to process private data because its terms and conditions were too ambiguous.

The regulator agreed. In the first big case to be decided under the new regulations, CNIL ruled that Google had breached the requirement for transparency. If customers wanted to find out how their data was used – especially for the business' geo-tracking service – they would have to click through five or six different pages on the company's site. Even then, some of that information was "not always clear nor comprehensive." In addition, CNIL said that because the company used the data for an array of services, Google's legal basis for processing it for each individual service was too opaque to the customer.

The regulator also found fault with Google's consent procedures for targeting customers with personalized ads. It complained that users had to go into the "more options" menu to modify how their data would be used – the consent box there was already pre-ticked. More importantly, CNIL noted that in creating an account, the user was effectively agreeing to a range of data processing by the company – involving ads personalization, speech recognition, and more – which were all covered by a single agreement. "GDPR

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

provides that the consent is 'specific' only if it is given distinctly for each purpose," CNIL concluded.

GDPR IS JUST THE START

While Google has appealed the case to France's top administrative body, the Council of State, CNIL's train of logic provides an indication of how regulators are interpreting key aspects of GDPR for organizations based anywhere in the world and how they are applying fines. More than that, GDPR is likely to change the way organizations handle private data globally. No wonder internal auditors who felt they had crossed the finish line when GDPR went live are realizing they have just begun the race.

"Many U.S.-based organizations wish that they would have started their GDPR compliance efforts earlier," says Jan Hertzberg, independent privacy consultant and adjunct professor at DePaul University in Chicago. Last year, many of them focused on updating their privacy policies and notices just before GDPR requirements went into effect. In the year to come, they plan to prioritize enterprisewide, GDPR risk assessments "to identify their greatest risks" and perform GDPR governance audits, he notes.

This new focus on data privacy is timely because GDPR's underlying philosophy is finding its way into new regulations around the world: Customers have to specifically opt into services, their consent over data processing has to be explicit, they have a right to know what data organizations hold and how they use it, and organizations must have rapid response processes to notify regulators and customers of serious data breaches. In the EU, for instance, the provisions of GDPR will be extended to electronic communications by a new e-Privacy Regulation, which is expected to come into effect later this year. These rules will govern how organizations can send out unsolicited marketing emails and text messages, will enable web users to set their cookie preferences on their browsers, and will stiffen up confidentiality rules for internet businesses.

Further afield, China last year introduced a slew of regulations on cybersecurity, data protection, and cross-border data transfer with distinctive GDPR-type features. And in the U.S., the California Consumer Privacy Act of 2018, which takes effect in 2020, features opt-out clauses, transparency rules, and rights for customers to be forgotten similar to those contained in GDPR.

Internal auditors are working to better understand the regulators' approach in balancing advice and punishment. And some are busy building networks within and outside of their organizations to help them understand the rules and what they mean to their enterprises. And while increasing their IT competencies is likely to be important, getting to grips with strategic issues is key.

REGULATORS' APPROACH

GDPR applies to all businesses that hold the personal data of citizens of the EU, making businesses outside of Europe potentially subject to European rules. In this year's Google case, CNIL made an important distinction that is likely to carry weight for complaints involving U.S. companies and others based outside of Europe. Despite the fact that Google's European headquarters are in Dublin, Ireland, CNIL brought the case against the U.S. parent Google LLC. It ruled that because the U.S. office had the final say on how data collected through its Android app was used, the U.S. parent was legally responsible for complying with GDPR. Any fine is calculated, therefore, on the parent company's turnover. In 2017, Google LLC had turnover of $110 billion, so the company could have been fined $4.4 billion, rather than the $57 million imposed by CNIL.

The U.K. regulator, the Information Commissioner's Office (ICO), says fines do not represent the biggest threat to organizations from GDPR. It says the idea that there will be massive fines is "myth No. 1" when it comes to understanding how regulators are implementing and interpreting their new powers. "In terms of powers and sanctions, the ICO aims to educate and support organizations in fulfilling their responsibilities in relation to data protection," says Debora Biasutti, lead communications officer for the ICO. "Issuing fines has always been, and will continue to be, a last resort."

> Regulators are working with businesses to help them comply, but are prepared to fine them for perceived noncompliance.

At the time of publication, the U.K. could potentially leave the EU without a formal set of agreements to govern how data on citizens is used between the two territories. If that happens, the U.K. will be covered by the 2018 Data Protection Act, which enshrines most of the provisions of GDPR into U.K. law.

Early indications are that regulators are working with businesses to help them comply but are prepared to fine them "proportionately" for perceived

Only 20% of businesses surveyed after the May 25, 2018, deadline say they were GDPR compliant, according to TrustArc's GDPR Compliance Status report.

noncompliance. How regulators are seeking to help organizations can be seen by a series of cases involving much smaller businesses than Google.

In December 2018, for example, CNIL closed a GDPR consent case with a small French ad tech firm called Fidzup. According to the online magazine *TechCrunch*, Fidzup worked with CNIL to create a longer consent form so that customers could opt into, or out of, every service it offered individually, which echoes CNIL's approach to Google.

"Now, okay, we have something between the initial asking for the CNIL—which was like a big book—and our consent collection before the warning, which was too short with not the right information," Fidzup CEO Oliver Magnan-Saurin told *TechCrunch*. The amended consent form is still a long read, he concedes. The company also had to alter the way its technology worked so that, for example, the app and its geolocation features worked even if the data did not go to advertisers when the user opted out.

SLOW BURN

It is not clear whether internal auditors have fully grasped the extra-territorial reach of GDPR, according to recent IIA research. The 2019 North American Pulse of Internal Audit found that while 70 percent of chief audit executives (CAEs) surveyed were highly concerned about suffering reputational damage from privacy issues, only 29 percent expressed high concern about compliance with GDPR—although that concern grew to 62 percent among large organizations. "This could reflect some misunderstanding of how and when these new data protection and privacy rules apply," the report says. The fact that the rules are not based on the location of the organization, but on the location of the customer whose data is being gathered, could have led some CAEs to believe their businesses are not affected, the report suggests.

Hertzberg says organizations' apparent slowness to respond to GDPR requirements may be attributed in part to a lack of knowledge of GDPR requirements along with lack of clarity as to how to comply. He is somewhat critical of what he sees as the shortage of attention the EU has paid to educating businesses outside Europe. "Since this is so obviously a worldwide phenomenon, European regulators would do well to consider the foreign players more," he says.

"Lack of awareness of GDPR requirements is a critical issue for organizations' management, staff, and board," Hertzberg adds. Internal auditors and compliance professionals often struggle to get those stakeholders to pay attention to what seems to be a European issue. "Now that the newness of GDPR has worn off, there is a concern that these requirements will get even less attention in the future," he explains.

Hertzberg notes that some internal audit management—for example, CAEs and directors of internal audit—may be reluctant to hire cybersecurity and privacy specialists for their departments. Instead, they have chosen to collaborate with their own general counsels, chief information security officers, and chief privacy officers to help them come to grips with what the regulations mean in practice. They also have enlisted assistance from third-party consultants.

Overall, CAEs have put focus on cybersecurity and privacy awareness so those with operational responsibilities clearly understand that they must "own" the data they collect and use. In doing so, they will better understand the need for and the issues around the retention and protection of personal data. More problematically, he says, businesses have been less clear about which named person is ultimately

> "Since this is so obviously a worldwide phenomenon, European regulators would do well to consider the foreign players more."
>
> Jan Hertzberg

> "Internal audit needs to help the business understand whether it is leveraging [data] as well as it should."
>
> Dominique Vincenti

“If internal audit has a good seat at the table, it can be a sounding board for both executive management and the audit committee.”

James Reinhard

responsible for the data that the organization owns.

“Compliance requirements, like GDPR, are forcing changes in the way that data is handled in many organizations,” Hertzberg says. “For CAEs, it is not just about data privacy, but data integrity throughout the business. That will mean internal auditors pay more attention than ever to data and become more data-centric in their approach to providing assurance.”

BUSINESS ISSUES

Dominique Vincenti, CAE at Uber and former vice president of internal audit at Seattle-based Nordstrom, says the initial risk for the department store business compared to larger online retailers was thought to be minimal because the proportion of shoppers based in Europe that use its online services is relatively small. “We used the opportunity to energize management around the topic because we felt that if it is not specifically GDPR, it is going to be something else that is GDPR-like,” she says.

Sure enough, a few months after GDPR took effect, California passed its own consumer protection laws. Vincenti says she would not be surprised if similar federal laws were in the pipeline. “California is significant to all U.S. businesses,” she explains. “If you are going to comply with its GDPR-like provisions, you are not just going to adapt your systems to only do so for your customers in California because it would be too difficult to segregate your customers. You just go with the highest common denominator.”

As GDPR-style regulations become more prevalent, businesses may need to rethink their strategic plans.

Vincenti says she expects most internal auditors will be ahead of the game when it comes to understanding the significance of such regulations. First, most will understand that the majority of organizations have poor data governance processes in place, so GDPR provides an opportunity to start addressing how businesses manage and govern data effectively. Second, those data governance weaknesses make GDPR a business issue, rather than a technology issue. “Internal audit needs to help the business understand whether it is leveraging and protecting this crucial asset as well as it should,” she says.

MODELS AND STRATEGY

As GDPR-style regulations become more prevalent, businesses may need to rethink their strategic plans, says James Reinhard, audit director at Simon Property Group in Greenwood, Ind. For example, instead of modeling an online initiative to contain data in a centralized server, a company may need to devise a more disbursed, decentralized model where it retains data in various countries because some of its target jurisdictions may prohibit cross-border data transfers. This, in turn, could affect the cost, reach, and viability of such projects.

“If internal audit has a good seat at the table, it can be a sounding board for both executive management and the audit committee, and it can assess how well the changing environment is being monitored by management,” he says. “If such alignment with management is not there, this is going to be an increasing problem for internal audit.”

Reinhard says CAEs may strengthen their IT competencies to enable them to conduct more sophisticated data privacy reviews, tracking and protecting such data as it flows through increasingly digitalized businesses.

“Internal audit will need to rely on the company’s legal counsel to provide guidance on interpreting what is the use

944 data breaches led to **3.3 billion** data records being **compromised** worldwide in the first half of 2018, according to the most recent Gemalto Breach Level Index.

of a specific set of data and the manner in which it must be secured," Reinhard says. "Naturally, if the company's legal interpretation is incorrect, then internal audit's opinion on attesting to compliance could be incorrect, too." Expanding internal audit's professional network can enable it to benchmark and find ideas that can be brought back into the organization, he adds.

FINDING MEANING

Regardless of where they are based, many businesses are struggling to understand what GDPR means in practice, says James Castro-Edwards, a partner at the London law firm Wedlake Bell. "We've heard of organizations issuing hundreds of pages of information in response to subject access requests when that is not what the law required them to do," he explains. There is a similar trend in reporting minor data breaches where the affected information is either low risk—people's names and addresses—or where it has been suitably encrypted and protected.

"Internal auditors are going to have to focus a lot more sharply on data protection compliance," Castro-Edwards says. That could include providing assurance on the business' understanding of materiality so that management is not wasting time over-reporting. The ICO has commented on the widespread over-reporting of personal data breaches since GDPR took effect. Many incidents have been reported on a cautionary basis, while the mandatory obligation to maintain a record of incidents—including an explanation of any decisions not to report incidents—may have been overlooked.

Castro-Edwards says regulatory enforcement action will gradually help businesses understand GDPR better. But fresh legal risks are still emerging.

Last year, the U.K. supermarket Morrisons found itself on the end of group litigation—or class action as it is known in the U.S.—brought on behalf of just over 5,500 employees. The plaintiffs were among 100,000 Morrisons workers whose personal details were released on the internet by a disgruntled former employee. In what could be the first of many such cases, a U.K. lawyer brought the action following a relatively recent development in the common law that established the principle that people affected by a personal data breach may be able to claim compensation for pure distress.

"It is early days, but this could become as big a risk for businesses as ICO enforcement activity, because of the number of individuals typically affected by a high-profile data breach," Castro-Edwards says. "Each affected individual need only claim a small sum for distress for the potential damages to mount up to a significant sum."

That could mean that a U.S. company holding data relating to U.K. customers could find itself caught up in a class action. "The fact of the matter is that the ICO and other regulators have limited resources," he says, "but any lawyer with the time and energy could bring this type of claim on behalf of a large number of individuals following a personal data breach."

Perhaps the key lesson of GDPR for internal auditors is that the new regulations not only changed the rules on data privacy and processing, they changed the game. It is a game where the winners will have good data governance and pay close attention to how the rules are developing globally. Internal auditors who have strong networks across the business and beyond will be able to support the board on how GDPR may impact both operations and strategy. They will, in short, be a key player on the team.

ARTHUR PIPER *is a writer who specializes in corporate governance, internal audit, risk management, and technology.*

> "Internal auditors are going to have to focus a lot more sharply on data protection compliance."
>
> James Castro-Edwards

IIA Training Stations
TRAINER
PLATFORM
ON-TIME
IIA ONDEMAND 24/07
IIA ON-SITE 09 TO 05
IIA IN-PERSON 09 TO 05
I ONLINE 12:00

The UPSIDE of risk

Internal auditors can provide greater value by also focusing on the positive.

Basil Orsini

Internal auditors characteristically interpret professional requirements to contribute to organizational risk management as helping senior management address weaknesses and threats to achieving the organization's objectives. The tendency to focus on downside factors that can actually or potentially impede organizational success is well-established and provides value that must continue to meet professional and stakeholder expectations.

But what about the organization's strengths and opportunities and their contribution to organizational goals? The concept of *positive auditing*, an approach that extends risk-based analyses and plans to improve strengths and opportunities, can enhance the value of independent assurance. While a typical internal audit provides assurances on downside organizational weaknesses and threats needing to be addressed, positive auditing provides assurances on upside organizational strengths and opportunities that need to be sustained.

Risk-based plans should include assurances on strengths, opportunities, and upside factors deemed critical to achieving organizational objectives. Importantly, this expansion complies with the current Definition of Internal Auditing and mandatory requirements of the International Professional Practices Framework (IPPF). Positive auditing enhances the organization's reputation by addressing the interests of the organization's stakeholders on what is working, as well as identifying areas needing improvement.

A SHIFT IN APPROACH

Shifting focus to strengths is consistent with innovations in the fields of social behavior. In 1998, after more than 100 years of primarily addressing the negative aspects of individual and social behaviors, the psychology profession formally expanded its scope to include the now burgeoning field of positive psychology. As noted by C. R. Snyder, Jennifer Pedrotti, and Shane Lopez in their book, *Positive Psychology: The Scientific and Practical Explorations of Human Strengths*, "positive psychology offers a balance to this previous weakness approach by suggesting that we also must explore people's strengths along with their weaknesses. … Positive psychology seeks a balanced, more complete view of human functioning."

By making a similar enhancement to how it sees and promotes itself, and how it is seen by its stakeholders, internal audit offers a more balanced and complete orientation to the assurance paradigm, which is a new area for service innovation and professional growth.

Internal auditors have taken initiatives to provide more balance in their reports by including positive findings for engagements.

BALANCED ENGAGEMENT REPORTING

Internal auditors have taken initiatives to provide more balance in their reports by including positive findings for engagements that normally focus on downside issues requiring improvement. This added balance demonstrates a greater understanding of business operations by internal auditors, motivates managers by recognizing where their efforts are showing results, and, consequently, encourages greater acceptance to address recommendations for improvement. Positive auditing builds on these initiatives and benefits by designing risk-based plans and engagements from the outset that consider the provision of high levels of assurance on positive areas deemed critical to organizational success within the domain of internal audit.

MORE COMPLETE RISK ANALYSES

The IPPF defines *risk* as "the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood." This definition is not limited to downside uncertainties; it also includes upside uncertainties, such as opportunities for gains.

The concepts of risk and risk management applied by internal auditors characteristically focus on addressing adverse uncertainties that are likely to negatively impact the achievement of organizational objectives. The orientation toward negative risk may be partly explained by the desire to minimize audit risk, such as the risk of making inaccurate assessments. As organizational weaknesses and threats often are known or suspected, there is less risk in accepting an internal audit and its recommendations. Because management makes decisions involving both upside and downside uncertainties, internal audit's risk analyses should be more comprehensive, leading to the development of more complete analytical tools and critical thinking.

MORE COMPLETE RISK-BASED INTERNAL AUDIT PLANNING

With positive auditing, risk-based audit planning broadens the scope of risk

The No. 1 mandate for audit committees is to understand and consider risks that could affect the business and its reporting, Protiviti's 2019 Setting the Audit Committee Agenda reports.

assessments to consider strengths and opportunities critical to the organization and where independent confirmation adds value. It brings consultations on internal audit plans more in line with management's interests in what is working and where independent assurances address the interests of external stakeholders. There is likely to be wider coverage and fuller alignment with the organization's business priorities.

There are occasions when independent evaluation and confirmation by internal audit of organizational strengths and weaknesses adds value. Consider three internal audit domains—organizational governance, risk management, and controls processes—which in the examples shown are not given priority in internal audit plans because there are no indications of significant adverse risk.

Organizational Governance This domain can benefit from assurances on organizational opportunities and strengths, as well as threats and weaknesses. Internal audit's objectives might be to:

- Ensure the organization appropriately administrates complaints concerning social and personal behavior.
- Ensure the integrity of positive performance information supporting year-end bonus payments to management.

Risk Management This domain benefits from oversight that provides comprehensive, validated information. The internal program of risk management considers strengths and opportunities, as well as weaknesses and threats to organizational success. Internal audit's objectives might be to:

- Ensure the robustness of the strengths and opportunities reported across the risk management program.
- Ensure the quality of due diligence activities in support of significant organizational initiatives and decision-making.

Examinations of Control Processes This domain provides operational oversight to keep the organization on track in achieving its objectives. Control processes adapt to evolving organizational needs. Internal audit's objectives may be to:

- Ensure the continued relevance and quality of performance standards and information relied on by senior management.
- Ensure the continued cost-effectiveness of systems of internal oversight.

These examples show where positive auditing might provide value-added assurance to the organization's stakeholders, even when the internal audit program and engagement plans are not expected to make material recommendations for improvement. The expanded scope into positive areas has the additional benefit of increasing internal audit coverage to find possible fraudulent behavior within the organization.

> Positive auditing brings consultations on internal audit plans more in line with management's interests in what is working.

THE CASE FOR POSITIVE AUDITING

Positive auditing broadens the range of internal audit assurance services by enhancing systematic consideration of upside factors—organizational

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

strengths and opportunities—in support of achieving organizational objectives. It provides a direction for service innovation and professional growth within the current IPPF by addressing upside risks and confirming what is working—both of which are deemed critical to organizational success.

It also contributes to organizational improvement by enhancing due diligence of management oversight and confirming the strengths in areas deemed critical to success. Internal audit processes increase analysis and attention to critical factors in the area being examined by all concerned. Should the examination disclose unexpected areas for improvement, management will have shown itself to be proactive and diligent in its pursuit of organizational performance. Either way, the confidence of external and internal stakeholders in management oversight is increased.

> Positive auditing can enhance the paradigm of the profession, expand assurance services, and enable us to tell new stories to our stakeholders.

Positive auditing also provides an opportunity to enhance the paradigm of the internal audit profession, expand the range of assurance services in risk-based plans, and tell new stories to our varied stakeholders. The internal audit community should consider the matter together, consult with stakeholders, and determine the extent to which positive auditing offers a viable direction for innovation in the profession.

BASIL ORSINI, CIA, CGAP, CRMA, CFE, *is a recently retired government auditor in Ottawa.*

AUDITING THE SMART CITY

Increasingly sophisticated municipal technologies introduce a host of risks that must be addressed.

Russell A. Jackson

As cities aggressively adopt "smart" technology—especially in the very public-facing transportation and safety arenas—municipal auditors will increasingly find themselves facing a new version of a familiar risk: cybersecurity. The underpinning of Internet-of-Things (IoT) connectedness that makes smart tech so smart is also its Achilles' heel, offering hackers access, on a vast scale, to all kinds of complicated technologies—and the people they affect. And countering that risk may require new internal audit skills and tools.

When the technology works, smart sensors create massive amounts of data that trigger mechanical responses: roadways charge electric vehicles as they pass above; connected cars find the best parking spots. But cybercrime experts take smart tech risks—and their implications for municipalities—quite seriously, painting a dark future portrait in the event things go awry. What happens, for example, if cybercriminals made every traffic light in a city green at the same time or scrambled the entire grid's color cycles during rush hour? What if they completely shut down the city's smart power grid? What if an attacker targeted water and sewage systems,

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

tampering with automated meters that detect and respond to flood conditions?

Auditors take those risks seriously, too. "The benefits that smart and emerging technologies can deliver are accompanied by multiple new risks," says Tonia Lediju, chief audit executive (CAE) for the City and County of San Francisco. "We need to ensure that cities have the right security governance, processes, and controls in place."

SMART CITY BY THE BAY

In San Francisco, there's a lot of smart tech to audit. Lediju says it's one of the leading smart cities globally, and it's working on even more smart mobility solutions—often in partnership with private companies or with the U.S. federal government. Initiatives include smart traffic signals, an electronic toll system with congestion pricing, and autonomous electric shuttles to Treasure Island in the San Francisco Bay. The city also uses smart parking meters that change prices according to the time and day of the week.

Lediju says her auditors tackle the new risks of smart tech head-on. The City Services Auditor Division assists the various city departments affected by new transportation technology, for example, in understanding the risks, monitoring the application controls designed to rein them in, and crafting preventive responses. Lediju says her team's annual work plan includes auditing new technologies when deemed necessary, based on a risk assessment.

The division works closely day to day with the City and County of San Francisco's Department of Technology, its Committee on Information Technology, and the departments adopting new technologies to ensure all risks are managed adequately, before adoption, Lediju says. She follows three key steps: understand the pipeline of emerging technologies being considered, identify risk trends, and help departments actively manage risks as they navigate relevant regulations.

In the cybersecurity space, the City Services Auditor Division "identifies systems' vulnerabilities and risks through penetration and assessment tests, and recommends remediation," Lediju explains. Testing encompasses several areas, including cybersecurity framework adoption, security awareness training, IT governance, systems and network security, and business continuity.

"We also contribute insight gleaned from our extensive scope of work to help departments evolve and improve their strategies and protocols to better prepare for cyberattacks," Lediju adds. Her team's work is based on the Cybersecurity Framework Core Functions outlined by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST): identify, protect, detect, respond, and recover. The City Services Auditor Division, she notes, also makes recommendations based on the CIS Controls and CIS Benchmarks guidance developed by the Center for Internet Security (CIS). "The CIS recommendations highlight for clients the numerous opportunities for control and process improvements or other enhancements that could ultimately increase their effectiveness in managing data security and fulfilling the organizations' missions and goals in serving the city," Lediju says.

> **Lediju says her team's annual work plan includes auditing new technologies.**

SWEDEN'S SMART TECH

At Sweden's Borlänge-based Trafikverket—the Swedish Transport Administration—the audit unit also gets involved early on, says Peter Funck, CAE. "The Agency," as he calls it, is the national government authority responsible for public roads and railways; Funck's office focuses on the planning and development phases, which is where he says his unit delivers the greatest added value. Audit and The Agency, he adds, have learned to manage large software and infrastructure development projects in similar ways, meaning audit is involved "several times before coding starts, as well as before the first spade is put in the ground," Funck says. That's been the case with two of Sweden's key smart tech endeavors:

- » The European Rail Traffic Management System (ERTMS) is a major industrial project underway in the European Union, Funck notes, and Sweden is one of the early adopters in developing and implementing it. ERTMS is a safety system that "enforces compliance by the train with speed restrictions and signaling status," he says.
- » Sweden is also developing a national system for controlling and scheduling all trains that will integrate train operator scheduling. "It's one of the biggest software-based projects ever in the country," Funck says. "The project brings a lot of opportunities, but, of course, size and complexity imply challenges: Will it work? Is it safe?"

Funck points out that his unit audited both the ERTMS and national integration projects several times, before they

More than 75% of city leaders and other stakeholders worldwide say blockchain technology could help solve urban problems, according to a 2018 survey by SmartCitiesWorld.

were even deployed on a test basis. “Those audits had different focuses,” he says, “but the common denominator has been whether internal controls provide prerequisites to make it work and make it safe.”

The projects aren’t yet far enough along for after-the-fact performance audits. But Funck notes that, in all of his office’s smart tech projects, health and safety, including terror attacks, are the largest risk concerns. “Information security often brings those risks down to some kind of acceptable level,” he says. Indeed, Funck emphasizes that available information security technology in general is up to the smart tech challenge; the bigger problem lies in people and their roles in keeping smart cities humming.

Funck adds: “There is always a need for some kind of security and safety risk acceptance in developing business processes to balance with productivity requirements.” At the end of the day, he points out, “railroads and roads are safer if we remove all trains and cars.”

DATA AND PRIVACY SAFEGUARDS

Jim Thompson, city auditor in the Albuquerque Office of Internal Audit (OIA), takes smart tech in stride, too, though he’s also well aware of the risks it poses—including those related to cybersecurity. “OIA performs an annual risk assessment of the city, which includes consideration of the city’s information technology risk,” he says. “As the city increases its use and reliance on information technologies, including smart technologies, the risk of cybersecurity and data breach—as well as the liability risk—increase.”

The city’s Technology and Innovation Department maintains internal controls over IT and also uses outside experts for IT vulnerability risk assessments and intrusion testing. Thompson maintains in-house technology expertise on his team as well. One senior information systems auditor, he says, holds several IT certifications, including CISA, CITP, and ITIL v3 Foundation.

The City of Albuquerque, Thompson says, has implemented various smart technologies, including government document and data transparency, ride apps, enhanced wireless access, and online police services. Planned audit engagements assessing privacy concerns will target some of those enhancements. “Our annual audit plan this year includes an audit of all city systems and devices that contain personal identifiable information [PII],” Thompson notes. “Some of the city’s smart technologies will be included.”

Thompson says the audit will consider whether the city maintains a listing of all systems and devices containing PII and if it has controls in place to classify and safeguard PII correctly, including intake points, release and data sharing points, and storage. It will also examine whether individuals with access to the city’s computer environment are trained on and aware of their responsibility to safeguard PII and what to do in the event of a data breach. OIA will consider federal, state, local, and contractual requirements for PII and compare the city’s current practices with IT governance framework best practices recommended by ISACA’s COBIT framework, as well as NIST.

PROTECTING THE VISION

Chattanooga, Tenn., City Auditor Stan Sewell also points to cybersecurity risk associated with his municipality’s emerging technologies. And while it’s not the No. 1 priority, the city’s tech-focused initiatives provide ample reason to ensure online security issues are addressed. “It’s definitely a risk, but it’s more of a ‘black swan’ concern,” he says.

Chattanooga’s Smart City Division, which manages street lights and traffic signals, acknowledges that

“The benefits that smart and emerging technologies can deliver are accompanied by multiple new risks.”

Tonia Lediju

“Technical challenges may result from our [city’s] vision in cybersecurity, hacking, and privacy issues.”

Stan Sewell

VISIT the online version of this article on InternalAuditor.org for additional discussion of how smart technology can amplify risks facing municipalities.

"technical challenges may result from our vision in cybersecurity, hacking, and privacy issues." "Vision" in Chattanooga includes autonomous vehicles and robust vehicle-to-vehicle and vehicle-to-infrastructure communications. The city won a 2019 Smart Cities Connect Smart 50 Award, a global recognition of transformative smart city project work, for its Chattanooga Smart Community Collaborative research partnership.

Sewell's primary concern is supervisory control and data acquisition (SCADA) systems, composed of computers and both wired and wireless data communications modules that provide remote access to and control of a city's infrastructure processes. "SCADA systems are vulnerable to cyberattacks," he says, "which are occurring with an increased frequency." A cyberattacker could gain remote control of the city's water treatment, for example, "commanding the release of wastewater or sending false pressure sensor data, resulting in a catastrophic failure of water pumps and controls." Sewell adds: "The various smart technologies increase the number of potential access points to enter the city's systems to gain access to other areas."

"Decision-makers value our input. ... We need a way to assess and report on emerging technology."

Amanda Noble

Selecting a particular technology to audit depends on the risk posed by the new technology as compared to other risks facing the city."

Andrew Keegan

TRIED AND TRUE

In some municipalities, the audit function's treatment of smart tech doesn't differ much from how it handles other city initiatives. Smart tech constitutes a largely routine subject, for example, for the City Auditor's Office in Kansas City, Mo.

City Auditor Douglas Jones says he is aware of many of the city's initiatives, one of which earned Kansas City a 2019 Smart 50 Award; plus, he knows smart tech is "timely and topical" and that it poses some reputation risk, as well as risks related to IT and operations. But from his perspective, newness can work against a program's auditability. "It often makes little sense to audit a program with no track record," he says. "And there's always risk with a new program."

Indeed, smart tech, Jones emphasizes, is "just one more thing that would be in our universe of potential audit topics. We cover everything from airports to the zoo, and we don't put a specific emphasis on one thing or the other."

Austin, Texas, another 2019 Smart 50 Award recipient, also places high priority on leveraging tech. In fact, Assistant City Auditor Andrew Keegan says Austin is trying to use its technology to help save lives. "Austin is committed to a Vision Zero plan, which calls for zero fatalities or serious injuries resulting from vehicle collisions by 2025," he explains. "Part of that plan is focused on implementing new technologies."

But Keegan's team likely won't be involved until after those plans and programs have been implemented. "Selecting a particular technology to audit depends on the risk posed by the new technology as compared to other risks facing the city," he says. "This is our practice regardless of the topic." Indeed, right now, his office is conducting an audit related to motorists' well-being. "While part of that project includes reviewing the implementation of new technology," he comments, "the audit is focused on the general issue of traffic safety."

Amanda Noble, city auditor in the City of Atlanta's City Auditor's Office, notes that Atlanta has implemented smart mobility tech, but she, too, says the audit function didn't have a role in assessing risk on the front end. "As the city was implementing the technology, we became aware of it and went to a demonstration," she says. "But we looked at the data the city was connected to and its potential uses in risk assessments and

Denial of service and malware/ransomware are the types of smart infrastructure attacks that concern security and risk professionals the most, according to ISACA's 2018 Smart Cities Survey.

DOWN THE PIKE

For municipal auditors who are not engaged to audit their city's smart tech right now, there's a good chance they will be soon. Indeed, Kansas City, Mo.'s Chief Innovation Officer Bob Bennett declared last year at the Smart Cities Connect Conference and Expo that municipalities that don't get on the smart tech bandwagon soon will find themselves part of a "digital Rust Belt."

» 66 percent of cities say they're investing in smart tech, according to a 2017 report from the National League of Cities called Cities and the Innovation Economy: Perspectives of Local Leaders; one-fourth of the rest are looking into it.

» International Data Corp. reported in January that worldwide spending on smart cities initiatives would reach $95.8 billion in 2019, an increase of 17.7 percent over 2018; by 2021, the total could hit $135 billion. Singapore, New York, Tokyo, and London are expected to invest more than $1 billion each this year, IDC added; the applications receiving the most funding are fixed visual surveillance, advanced public transit, smart outdoor lighting, and intelligent traffic management.

» IoT Analytics said late last year that there were 17 billion connected devices worldwide; the number of IoT devices – excluding smartphones, tablets, laptops, and fixed line phones – was pegged at 7 billion. "The number of IoT devices is expected to grow to 10 billion by 2020," the firm points out, "and 22 billion by 2025."

» Mobility is the most common area for smart tech investment, according to the National League of Cities report. Other key applications include lighting solutions, security, and utilities management, according to the McKinsey Global Institute 2018 report, Smart Cities: Digital Solutions for a More Livable Future.

audit work. We hadn't thought about auditing the technology itself."

Would it help? "I think it would," Noble says. She notes that her team has assessed controls on financial systems installations, but "possibly because smart tech is not financial data, the audit function has not been asked to play a role." Stakeholders viewing the profession as dealing primarily with financial information can be frustrating, she adds, in the face of internal audit training that emphasizes the importance of foresight in all areas of the enterprise.

"So much of our role is looking backward," Noble says. "There's not really a process for emerging risk, unless we do it as one-offs. There's nothing systematic." She adds that resource constraints limit the audit function's ability to tackle emerging issues, so new risks may not be audited until nearly a year has passed. She'd like to do more.

"Decision-makers value our input," Noble emphasizes. "We need a way to assess and report on emerging technology."

EXPANDED SERVICES, NEW SKILLS

Lediju sees a balance between tried and true audit services and helping organizations see around the corner. "We'll need to remain focused on our existing foundation of auditing standards and principles to detect internal control weaknesses and fraud risks," she says. "But the profession must be ready to take on more of an advisory role and help cities keep pace with and get ahead of emerging risks, maintaining its unique perspective on people, processes, and governance when striving to strengthen its risk management programs."

Because of the specialized knowledge required for new and smart technologies, she adds, internal auditors who possess a mix of business and technology skills will be needed. In fact, more of them will be needed. "Smart tech requires more internal audit resources because the pool of tools is constantly expanding and being used for various operations across government services," Lediju explains. As a result, she says, information and software oversight and accountability, including human and technology resources, become more necessary.

Internal auditors will need to adopt new tools and techniques, she adds, such as artificial intelligence and blockchain auditing and reconciliations, to increase continuous audit activities, rapidly pinpoint control gaps, and identify nonconformance and process improvement opportunities in real time. She says her office "currently relies on outside contracting and consulting services to keep abreast of the rapidly evolving trends and practices in technology, governance, security, and privacy relevant to the respective technologies."

Lediju adds: "With the requirements of continuing professional education and the goal to help businesses and government adopt best or leading practices, internal audit can remain a necessary and beneficial agent of change." Maybe, in fact, the profession could do more when it comes to smart tech.

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

It's

**Wade Cassels, Kevin Alvero,
Chris Errington**
Illustrations by Gary Hovland

Internal auditors need to shift the focus of audit reporting from their own priorities to those of the client.

The audit report was 25 pages long. The results didn't begin until page 16. Even worse, the audit's purpose was not revealed until well into the document. It appeared past the auditors' signatures, past a boilerplate that defined internal audit's role and established its independence, and past a description of the standards that were audited against. On the fourth page, 600 words into the audit report, the authors included just a single sentence that explained, albeit vaguely, why the audit had been performed.

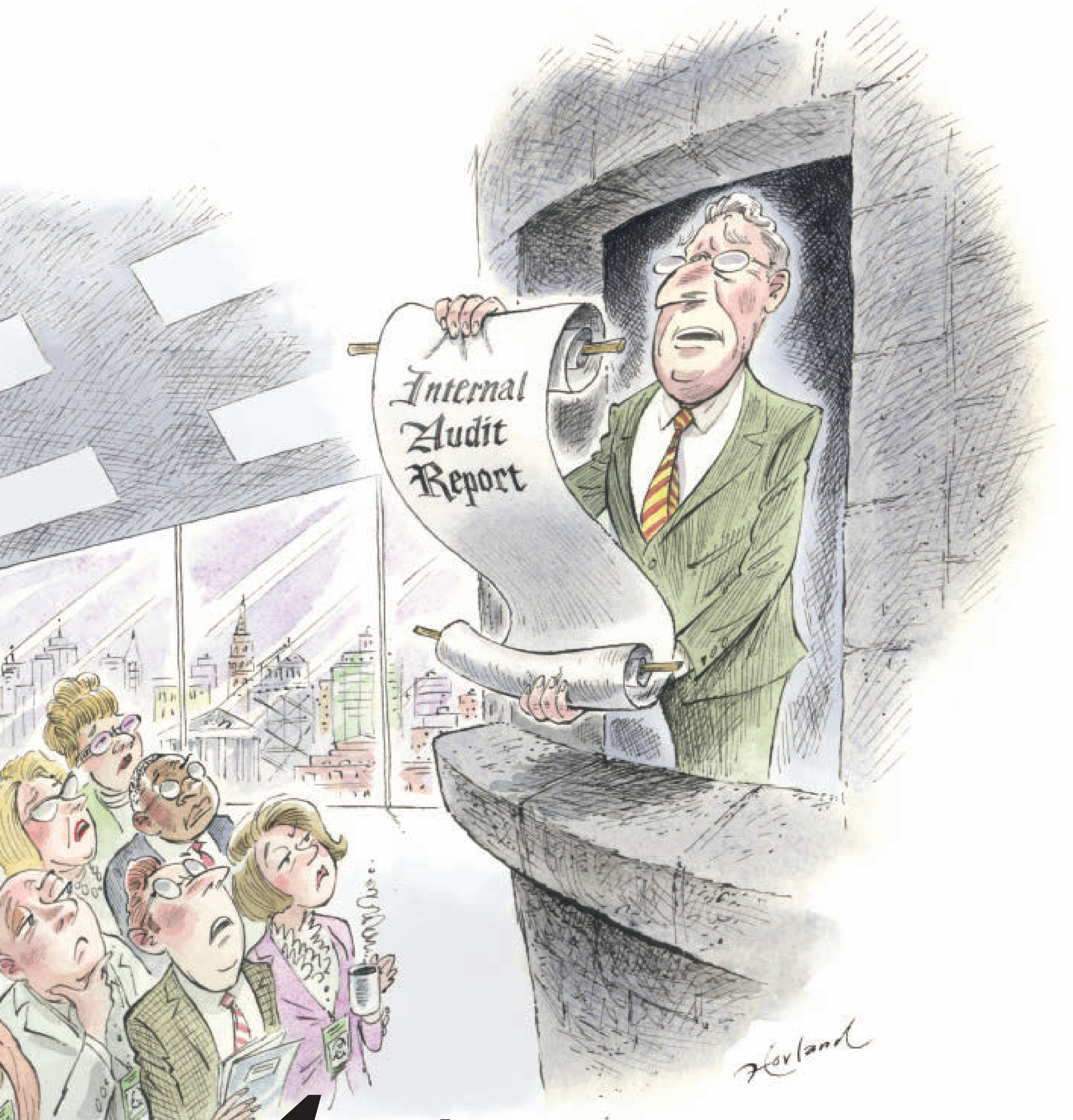
This is a true story, but it is not a tale of incompetence. Indeed, the audit itself represented superior work performed by a proficient and experienced practitioner. The anecdote instead points to a far-too-common breakdown between performing internal audit work and communicating results. It demonstrates audit reporting that focuses too much on the audit and the auditor, and not enough on the clients and their business objectives.

To fix this problem, auditors must train themselves to write audit reports with audience awareness. Putting that skill into practice, however, requires the support of audit management and the trust of the audit client. With these elements in place, auditors can produce reports that serve as a much more effective communication vehicle and provide greater value to their clients.

MAKING THE GRADE

In an article titled, "Understanding a Writer's Awareness of Audience," author and writing professor Carol Berkenkotter analyzed expert writers and the role of audience awareness in their composition process. Her work was inspired by "The Cognition of Discovery: Defining a Rhetorical Problem," a study by researchers Linda Flower and John Hayes that found experienced writers formed a mental image of their readers. College freshmen in the study struggled to think beyond the topic and content of their essays.

"Unlike real-world writing situations," Berkenkotter wrote, "which confront the writer with a variety of rhetorical situations and audiences with differing



not about you!

needs, school writing demands that the student write for a single authority, the teacher." As a result, success in the writing process is determined by the student's ability to demonstrate his or her expertise on a given subject to this authority figure.

Although professional auditors have left behind the classroom *setting*, reverting to a classroom *mindset* when writing audit reports can easily result in a focus on demonstrating the auditors' own authority. Reports produced this way often fail to effectively communicate the audit's value or meet stakeholder needs.

Fortunately, writing with audience awareness is a skill that can be learned and developed. Writers who exhibit audience awareness, Berkenkotter found, engage in four main types of activities — as shown in "Audience Awareness" on page 45. Each activity is accompanied by a list of questions, shown in the right column. Berkenkotter suggests that with practice over time, addressing these questions becomes less of a process and more of a state of mind. "Professional writers automatically internalize their audiences; as they write, they ask themselves the questions that their readers might be expected to ask," she says. "In the process of being one's own reader, an expert writer is constantly revising [his or her] own work." This imagined audience, she adds, becomes the touchstone upon which the writer bases his or her decisions, including organization.

For audit stakeholders, understanding the results is more important than knowing how they were found.

STRUCTURE AND SEQUENCE

Audit report content should be organized by its importance to the audit client. Beginning the audit results only after pages of describing audit procedures, as the report cited earlier did, makes sense only to the practitioner who has been immersed in the engagement for months. For internal audit stakeholders, seeing and understanding the results is more important than knowing how the results were found.

As a practical guide, the content of a client-focused audit report should be prioritized by four main areas:

1. The reason for the audit, related to client business objectives.
2. The results of the audit and their impact on client business objectives.
3. Recommendations, if any.
4. Information about the audit process and the auditors.

Although this structure reflects the order of importance, it does not strictly dictate the sequence of the report. For example, some information about the auditors and the audit process may be interwoven throughout the document — auditors don't necessarily have to place it all at the end. What matters is whether the report is client-focused (as opposed to audit-focused) and whether it prioritizes the information most important to the clients.

Audit reports, in other words, should not all follow the same template. Decisions about what to include, what to leave out, and how to organize the report should be made based on awareness of the audience. Writing with audience awareness will help auditors overcome the task-oriented mindset that results in audit-focused reports. But to put this technique into practice, auditors must believe they are empowered to change.

CULTURE AND EMPOWERMENT

The audit report that tells stakeholders what auditors want to say is an artifact

Ia VISIT OUR MOBILE APP + InternalAuditor.org
to watch a video series on audit reporting.

AUDIENCE AWARENESS

Author and writing professor Carol Berkenkotter identified four main activities engaged in by writers who exhibit audience awareness. Internal auditors can apply each of these to improve their audit report writing.

ACTIVITY	WHAT THIS MEANS FOR AUDIT REPORT WRITERS
Analyzing or constructing a hypothetical audience	Conceptualize the report's audience. Who are they? What are their roles? What are their needs? What are their goals? Likes/dislikes? How do they perceive me?
Setting goals and naming plans aimed at a specific audience	Identify the intended takeaway from the report. What do you want the audience to understand? What do you want them to do? What is most important?
Evaluating content and style (persona) with regard to anticipated audience response	Consider how the audience will respond to the content and style of the report. Is the style appropriate for the audience? Is the style appropriate for the audit subject matter? Does the style affect whether the information will be received in a desirable or undesirable way?
Reviewing, editing, and revising for a specific audience	Systematically review and improve the text, keeping the audience in mind. Does it speak the language of the audience? Does it achieve its communication goals based on perceptions of the audience?

Adapted from Carol Berkenkotter's "Understanding a Writer's Awareness of Audience," *College Composition and Communication,* Vol. 32, No. 4 (December 1981), 388–399.

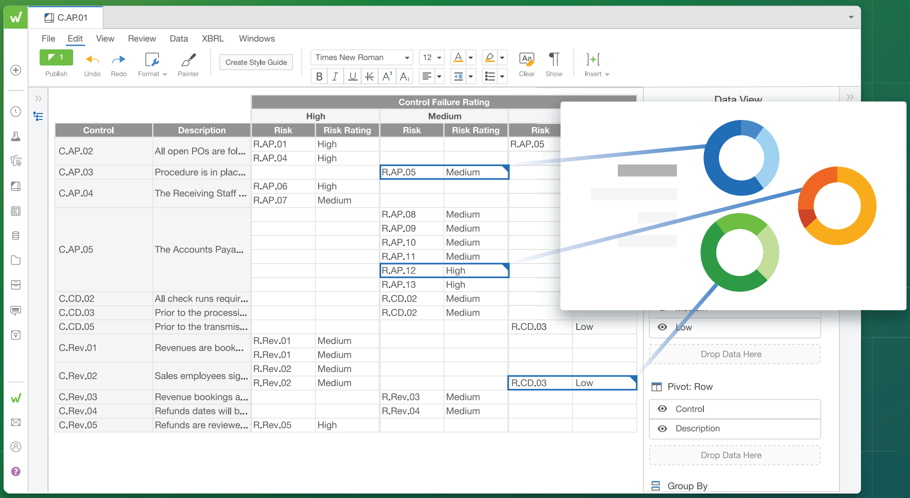
encountered by many new practitioners when learning the profession. Cultural subtleties, such as referring to the report with words like "deliverable" and "work product," reinforce the notion that the report's purpose is to document internal audit's execution of the engagement.

CAEs and audit managers must coach their staff to write audit reports that focus on the client's business objectives.

To change this mindset, audit managers and chief audit executives (CAEs) must begin to empower their staff members and require them to take a different approach to reporting. Regardless of how many articles they read or seminars they attend, practitioners will never change for the better if their audit department's culture includes an unspoken expectation that audit reporting involves filling in old templates. When CAEs and audit managers read audit reports that begin with, "Internal audit conducted a review of …" they must start sending them back and coaching their staff to write reports that focus on the client's business objectives.

In fairness, because the audit report typically serves as the primary method of documenting what happened in an audit, practitioners will naturally want to justify their value by demonstrating the volume and quality of the work performed. Rather than asking the auditor to merely suppress this inclination, audit managers can relieve the burden by giving auditors other outlets through which to communicate in detail about the rigor and quality of their work. For example, managers could simply meet with auditors to discuss the execution of a given engagement, allowing the auditors to discuss how much time they spent on it and any difficulties encountered, as well as revisit decisions that were made. These types of details—important to the audit process but too granular for the client—should be documented in the audit's workpapers for later reference. The documentation can help assure

Be confident.
Stay consistent.
Work together.



		Control Failure Rating					
		High		Medium			
Control	Description	Risk	Risk Rating	Risk	Risk Rating	Risk	
C.AP.02	All open POs are fol...	R.AP.01	High			R.AP.05	
		R.AP.04	High				
C.AP.03	Procedure is in plac...			R.AP.05	Medium		
C.AP.04	The Receiving Staff ...	R.AP.06	High				
		R.AP.07	Medium				
C.AP.05	The Accounts Paya...			R.AP.08	Medium		
				R.AP.09	Medium		
				R.AP.10	Medium		
				R.AP.11	Medium		
				R.AP.12	High		
				R.AP.13	High		
C.CD.02	All check runs requir...			R.CD.02	Medium		
C.CD.03	Prior to the processi...			R.CD.02	Medium		
C.CD.05	Prior to the transmis...					R.CD.03	Low
C.Rev.01	Revenues are book...	R.Rev.01	Medium				
		R.Rev.01	Medium				
C.Rev.02	Sales employees sig...	R.Rev.02	Medium				
		R.Rev.02	Medium			R.CD.03	Low
C.Rev.03	Revenue bookings a...			R.Rev.03	Medium		
C.Rev.04	Refunds dates will b...			R.Rev.04	Medium		
C.Rev.05	Refunds are reviewe...	R.Rev.05	High				

Connect people, processes, and data to gain control of internal audit and empower collaboration across the enterprise.

See Workiva solutions in action:
workiva.com/audit-video

workiva®

53% of audit functions communicate the organization's level of cyber risk, and efforts to address such risk, to management and the board, the 2019 North American Pulse of Internal Audit finds.

auditors that even though clients might not be apprised of process minutia, audit management understands and appreciates these details.

CLIENT TRUST

To make the transition from defensive audit reporting that focuses on process documentation to reporting that is proactive and focused on audience utility, internal auditors must also have the trust of their clients. One reason audit reports often contain excessive process detail is that practitioners worry clients may be resistant to, or suspicious of, the audit process — especially if the client might view the results as unfavorable. When this occurs, internal auditors focus primarily on defending their work and results rather than communicating what those results mean to the client's business.

To overcome this defensive mindset, internal auditors must constantly work to strengthen trust — in both the audit function as a whole and each of its practitioners, from one engagement to the next. If clients receive regular communication throughout engagements, understand that internal audit's mission is to help the business achieve its objectives, and have been educated about the audit process, they will be able to accept audit reports with trust, boilerplates and disclaimers aside.

IT'S ABOUT THE AUDIT CLIENT

Writing engaging audit reports that are suited to the needs of the individual client can be liberating for practitioners, but it also represents a challenge. Outside the safety zone of template-based reporting, auditors must make careful choices about what to include, what to exclude, and in what order to place information to maximize the client's perception of report quality and utility. However, the payoff for practitioners willing to undertake this challenge is enhancing their clients' understanding and appreciation of the value of internal audit.

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

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

CHRIS ERRINGTON *is a senior communications specialist at Nielsen.*

the MORE you say

Many audit committees are voluntarily disclosing information about their oversight and performance.

Craig G. Gallagher
Katheryn L. Zielinski
Douglas M. Boyle

Audit committees of U.S. publicly listed companies have had greater disclosure responsibilities since the U.S. Sarbanes–Oxley Act of 2002 took effect. Both the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) have established and enforced audit and disclosure guidelines, including rules for what audit committees must disclose to the public. But those required disclosures are limited in scope.

Recently, some audit committees have begun providing voluntary disclosure to improve transparency and give further insight into the committee's composition, activities, and decision-making processes. Voluntary disclosure provides additional context to mandatory SEC disclosures. Some audit committees may be disclosing more in hopes that it will discourage the SEC from expanding disclosure requirements. Moreover, shareholders and other stakeholders can benefit from more information about how audit firms are selected, compensated, and evaluated.

In light of this development, internal auditors need to understand which audit committee disclosures are required and become familiar with the voluntary disclosure trend. By engaging with the board and audit committee, internal audit can help shape opinions around which voluntary disclosures may benefit the organization and key stakeholders. Moreover,

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

it can give the board a better understanding of disclosure trends.

REQUIRED DISCLOSURES

The SEC has largely defined audit committee disclosure requirements since 1999. Historically, these requirements have been limited to descriptive information and select process assertions, which continued after the passage of Sarbanes–Oxley. Currently, SEC Regulation S-K, Item 407, requires the audit committee to:

- State whether the audit committee has a charter, and if so, provide appropriate disclosure.
- If the board deems an audit committee member is not independent, disclose the nature of the relationship that makes that individual not independent and the reasons for the board's determination.
- Disclose whether the audit committee has reviewed and discussed the audited financial statements with management.
- Indicate whether the audit committee has discussed with independent auditors matters required in AU section 380 of the PCAOB's "Communication With Audit Committees."
- Include that the audit committee has received a letter from the independent accountant, including written disclosures pertaining to accountant independence (per PCAOB regulations).
- Based on the appropriate review and discussions, provide a statement recommending that the audited financial statements be placed in the company's 10-K or annual report.
- Disclose member independence, including proof that at least one member is a financial expert.
- Provide the names of each audit committee member or those acting in the role of the audit committee.

Internal auditors can educate the audit committee on voluntary disclosure trends.

In 2015, the SEC issued a concept release on possible revisions to audit committee disclosures, but the SEC has yet to change its requirements. In a July 2017 address at the Economic Club of New York, current SEC Chairman Jay Clayton stated that several SEC initiatives are underway to improve disclosures to investors.

Internal auditors should evaluate whether management has adequate governance to ensure required audit committee disclosures are appropriately identified and made. Creating a disclosure matrix that contains categories of SEC required disclosures can ensure all SEC mandatory items are included in the audit committee's proxy disclosures.

VOLUNTARY BENEFITS

In addition to adhering to the required disclosures, audit committees often voluntarily communicate additional information to their stakeholders. A variety of organizations have advocated for greater disclosure in recent years. In his response to the SEC's Audit Committee Disclosure concept release in 2015, IIA President and CEO Richard Chambers noted that increased disclosure could support internal audit's stature, independence, and resources. It also could build trust with investors and other external users of financial information.

Deloitte's July 2018 On the Board's Agenda report notes that Standard & Poor's (S&P) 100 proxies "help to provide transparency into audit committee oversight activities." Also, a 2017 Deloitte report stated that "transparency

43% of audit committees disclosed their cybersecurity oversight role, and 40% discussed management judgments or accounting estimates in 2018, notes a Deloitte analysis of S&P 100 proxies.

VOLUNTARY DISCLOSURES RISING

The table below illustrates audit committee five-year voluntary disclosure trends for S&P 500, mid-cap, and small-cap companies. Although voluntary disclosure is up for all three categories, a higher percentage of large companies voluntarily disclose than smaller companies.

	S&P 500		S&P MID-CAP		S&P SMALL-CAP	
DISCLOSURE ITEM	2014	2018	2014	2018	2014	2018
Audit committee considerations in appointing audit firm	13%	40%	10%	27%	8%	19%
Length of audit firm engagement	47%	70%	42%	52%	50%	51%
Audit committee responsibility for fee negotiations	8%	20%	1%	5%	1%	4%
Discussion about nonaudit services' impact on independence	83%	83%	69%	78%	58%	75%
Criteria considered when evaluating the audit firm	8%	46%	7%	36%	15%	32%
Evaluation of the audit firm at least annually	4%	26%	3%	17%	4%	12%
Audit committee involvement in audit partner selection	13%	52%	1%	20%	1%	10%
Audit partner rotation every five years	16%	49%	3%	20%	4%	12%

Source: The Center for Audit Quality, 2018 Audit Committee Transparency Barometer

into the audit committee's oversight activities and performance can provide investors with a better understanding of both the audit committee's performance and the audit process."

In addition to transparency, EY's 2018 Report to Shareholders notes that although investors say they are confident in publicly listed companies' financial reporting, some are evaluating company-auditor relationships. Earlier, the firm's Audit Committee Reporting to Shareholders 2017 pointed out that stakeholders are looking closely at the board and audit committee's role in "supporting high-quality financial reporting."

Two separate publications from EY and the Center for Audit Quality (CAQ) highlight many potential benefits to a company in providing voluntary disclosure:

- » Increased transparency with key stakeholders.
- » Alignment of all stakeholder expectations, resulting in reduced conflict.
- » Trusting relationships among stakeholders.
- » Increased investor confidence in the board.
- » Increased investor confidence in financial earnings quality.
- » Increased investor confidence in the presence of corporate policies.
- » Ability to assess top management's decisions and behaviors.
- » Improved insight and assessment of the audit committee's decision-making process.

Internal auditors can educate the audit committee on voluntary disclosure trends—both overall and within their industry—and the potential benefits to the organization. They can add a voluntary category to their disclosure matrix to list potential voluntary disclosures for their organization to consider. To compile that list, they should consult current disclosure studies and research what S&P 500 companies and other organizations in their industry are reporting. Based on such findings, internal auditors can assist management and the board with recommendations on the extent and type of voluntary audit committee disclosures that their organization should make.

DISCLOSURE TYPES

The CAQ's 2018 Audit Committee Transparency Barometer report

KEYNOTE SPEAKERS

Lisa Osofsky
Director, U.K. Serious Fraud Office

Bill Browder
CEO, Hermitage Capital
Author of New York Times Best Seller
Red Notice: A True Story of High Finance, Murder and One Man's Fight for Justice

Bastian Obermayer
Investigative Journalist,
Panama Papers Recipient,
2017 Pulitzer Prize Winner
Süddeutsche Zeitung

ACFE GLOBAL FRAUD CONFERENCE

JUNE 23-28, 2019
AUSTIN, TX

LEARN NEW WAYS *Fraud* IS BEING COMMITTED
AND TACTICS to PREVENT, DETECT and DETER it.

Network WITH MORE THAN 3,000 FRAUD FIGHTERS

100+ EDUCATIONAL SESSIONS
including an
AUDITING FOR FRAUD TRACK

NEARLY 25% OF ATTENDEES ARE *auditors!*

EARN UP TO 40 CPE

STEP UP. *Stand Out.*

Visit **FraudConference.com** to register.

88% of Fortune 100 audit committees disclosed they are responsible for the external auditor's appointment, compensation, and oversight, up from 44% in 2012, according to EY.

provides insight into what companies are voluntarily disclosing beyond the SEC requirements. The barometer provides five-year trend data for four categories of "enhanced disclosure" for each S&P 500, mid-cap, and small-cap company:

- Audit firm selection/ratification.
- Audit firm compensation.
- Audit firm evaluation and supervision.
- Audit engagement partner selection.

The sampling frame used in the CAQ's report was the S&P Composite 1,500 proxy statements of companies in these indices at the end of the filing period. "Voluntary Disclosures Rising" on page 51 reveals an upward trend in nearly all analyzed voluntary disclosures between 2014 and 2018. This increase may be driven by two factors.

First, these areas provide insight into how diligently an audit committee is assessing the audit firm's independence. The SEC cites this responsibility as one of the most important duties of an audit committee.

A second factor may be a response to recent PCAOB Staff Inspection Briefs that have expressed ongoing concerns with audit firm independence. In December 2018, the PCAOB's Inspections Outlook for 2019 listed independence among its key areas of focus for inspections in 2019 and beyond. The board's August 2017 Staff Inspection Brief noted that some firms' systems of quality control did not provide enough assurance that their personnel understood and complied with independence requirements. Among the deficiencies were impermissible nonaudit services and instances where external auditors performed such services without the audit committee's preapproval.

Similarly, a 2018 proxy review by the Deloitte Center for Board Effectiveness found disclosures related to auditor independence increased 10 percent across a sample of S&P 100 companies that reported by May 31, 2018. Given these two factors, audit committees may be increasing voluntary disclosure to provide further assurance that they are taking appropriate action to ensure audit firm independence.

PRACTICAL IMPLICATIONS

With more audit committees opting to provide voluntary disclosures, internal auditors can provide valuable insights on the topic to their audit committee. Practitioners should periodically monitor the audit committee disclosures among the organization's competitors and any further action that the SEC may take on its 2015 concept release. Additionally, internal auditors should monitor annual publications from the CAQ, PCAOB Staff inspection briefs, and related applicable documents to both understand disclosure trends and provide necessary attention to them. Finally, internal auditors should inform clients that investors are evaluating the relationship between companies and audit firms. One way to communicate about this topic to investors is through voluntary disclosure. Ia

The PCAOB listed independence among its key focus areas for inspections in 2019.

CRAIG G. GALLAGHER, PMP, *is a doctor of business administration student at the University of Scranton in Pennsylvania.*

KATHERYN L. ZIELINSKI *is a doctor of business administration student at the University of Scranton.*

DOUGLAS M. BOYLE, DBA, CPA, CMA, *is accounting department chair and associate professor at the University of Scranton.*

Navigating expectations

Internal auditors can use a multifaceted approach to manage the diverse needs of stakeholders.

Jack Pelikan

Aesop's Fable, "The Miller, His Son, and Their Donkey," recounts the trio's perilous journey to the market where, along the way, the man and his son face various criticisms for each of their decisions. First, they are chided as foolish and wasteful for walking, and then lazy and cruel for riding. In a desperate attempt to quell the second criticism, they decide to carry the animal only to lose it in the river. The moral is that it is impossible to please everyone given the diversity of opinions, and that attempting to do so can be a fruitless endeavor.

This predicament also applies to internal audit functions. As the role of internal audit continues to expand, so does its stakeholder base and the level of expectations. But, like the onlookers from the fable, internal audit's broadening stakeholder base may value a variety of conflicting qualities. For instance, an organization's manufacturing department, which values efficiency and minimized downtime, may perceive internal audit's U.S. Sarbanes-Oxley Act of 2002 controls testing as valueless and disruptive to its operations, while the chief executives and external auditors may view such testing as

an invaluable barometer in their overall controls assessment.

In acknowledging that universal stakeholder approval is not always possible, an effective internal audit function also realizes that it can consistently act in the best interests of the organization and its core values, even if it leads to some dissatisfied stakeholders along the way. And while each organization's values are unique and there is no one-size-fits-all approach to stakeholder management, chief audit executives (CAEs) and their staff members can consider specific actions throughout the engagement life cycle while navigating widespread stakeholder expectations.

BEGIN WITH THE RISK ASSESSMENT

Regardless of the industry, organization, or department, all stakeholders face some form of risk and understand the need to manage it within acceptable levels. That said, disagreement on the nature and severity of risk is inevitable. While auditors are not expected to evaluate risk through the same lenses as their stakeholders, they can use the risk assessment process to engage stakeholders—such as through interviews and surveys—and as an opportunity to align future audits or projects with mutually agreed-upon risks. Further, to ensure stakeholders are on board with the risk ratings and evaluation criteria, auditors should use generally accepted risk assessment methodologies, such as The Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management–Integrating With Strategy and Performance.* Wherever possible, they should quantify the likelihood and potential impacts of such risks in lieu of using highly subjective, and often contentious, heat maps with high, medium, and low categorizations.

ALIGN ENGAGEMENT GOALS

Once the need for an engagement has been established by aligning it with mutually agreed-upon risks, internal auditors should set goals for the engagement and discuss them with impacted stakeholders before beginning fieldwork. Further, auditors can gain stakeholder interest by articulating the direct or indirect links between the proposed engagement and the accomplishment of departmental and organizationwide objectives. For example, an operational audit of an organization's shipping function should begin by evaluating the department's immediate and long-term goals, such as shipment of 100 percent of forecasted orders this month, quarter, and year, and the organizationwide objectives they support, such as greater customer satisfaction and improved profitability.

As a result, the engagement's goals should include identifying issue root causes and providing recommendations that will enable them to achieve their goals. When the department's goals conflict with, or do not align with, enterprisewide objectives, further dialogue with departmental and executive leadership may be warranted before beginning fieldwork.

OBTAIN BUY-IN

To promote a "no surprises" approach, internal auditors must proactively communicate engagement goals with their stakeholders and obtain consensus on scope and timing. While this practice seems obvious to many, its importance is sometimes overlooked. Auditors should use engagement proposals, scope documents, and kick-off meetings as a vehicle for engaging their stakeholders and establishing ground rules and expectations.

Furthermore, obtaining stakeholder buy-in requires not just discussing the engagement terms, but also communicating what's in it for them. While this message can be challenging, especially on a mandatory compliance audit, stakeholders are far more inclined to act as a partner when they are aware of the incentives. For example, instead of warning sales department leaders about the penalties for their team's noncompliance with company travel and expense policies, an internal auditor reviewing travel expenses can emphasize the benefits of cooperation during the audit, such as shorter audit duration, less disruption, and a reduction in audit findings. The audit also can point out the advantages of implementing the subsequent recommendations, such as greater management and monitoring of expenses and budgetary adherence.

STAY AGILE

While a robust engagement plan can set the tone and ensure the efficient allocation of audit resources, an internal audit engagement's—and department's—success is contingent on the team's ability to promptly adapt to change. According to The IIA's 2018 North American Pulse of Internal Audit, two-thirds of CAEs significantly value future agility, yet only 45 percent consider their departments very or extremely agile today.

The process to becoming agile can begin by leaving flexibility in the engagement plan, which can range from budgeting hours for responding to ad hoc requests, to continuously refining the plan after major milestones. In addition, audit teams need to establish a scope change management protocol with stakeholders up front to ensure changes to the original plan and scope are handled consistently.

USE ACCEPTED METHODOLOGIES AND BEST PRACTICES

To avoid irreconcilable differences of opinion, auditors can base their approach, evaluation criteria, and, ultimately, their conclusions on generally accepted standards. For instance, while assessing a company's IT password requirements, an auditor is likely to

TO COMMENT on this article, **EMAIL** the author at jack.pelikan@theiia.org

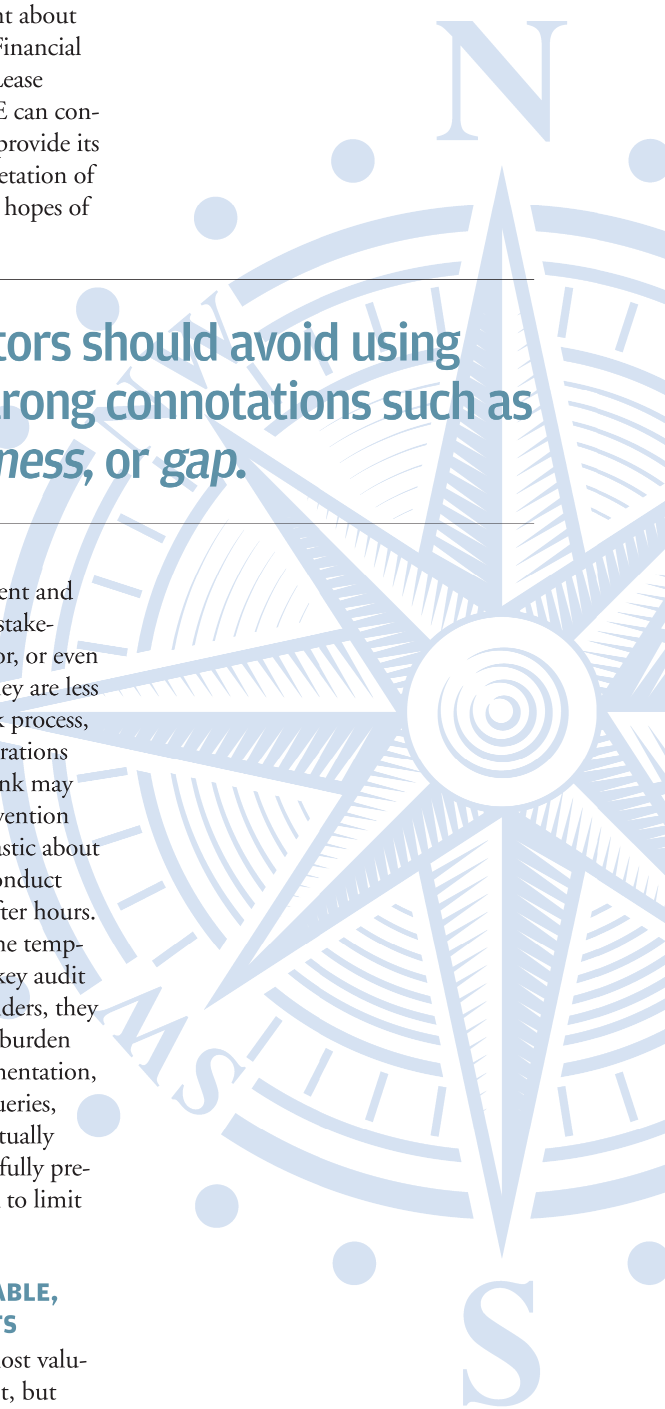
encounter stakeholder pushback and questioning by concluding that the password length requirements are weak or even noncompliant without attribution to a specific framework. On the other hand, if the auditor notes that the company's current password length requirement of five characters does not align with the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63 recommendation of at least eight characters, stakeholders are far less inclined to challenge the finding and more likely to accept the recommendation, especially if they also value the NIST framework and were apprised of the audit criteria earlier in the engagement.

REMAIN NEUTRAL

Regardless of the organization, interdepartmental conflicts or turf wars are inevitable, and by virtue of their authority, internal auditors often are petitioned by stakeholders to support a particular side. IIA Standard 1120: Individual Objectivity states, "Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest." While maintaining an objective mindset is critical, it can be far more challenging for internal auditors to appear neutral in the eyes of their stakeholders. In addition to abiding by the explicit requirements of neutrality, which include refusal of gifts and avoidance of workplace fraternization, internal auditors should refrain from being overly complimentary or critical of a particular stakeholder group in their interactions and in their reports. For example, internal auditors should avoid using words with strong connotations such as *failure*, *weakness*, or *gap* and replace them with more constructive terms such as *opportunity*.

In the unfortunate situation where a dispute arises between internal audit and a stakeholder, such as disagreements over regulatory interpretations, audit findings, or recommendations, CAEs should consult a mutually regarded third party as a mediator, whether it is another department, such as legal or human resources, or outside consultants. For instance, if internal audit and accounting have a disagreement about the interpretation of the new Financial Accounting Standards Board Lease Accounting Standard, the CAE can consult the external audit firm to provide its independent, objective interpretation of the standard to both parties in hopes of achieving greater alignment.

> **Internal auditors should avoid using words with strong connotations such as *failure, weakness*, or *gap.***



BE SELF-SUFFICIENT

While a thorough risk assessment and well-articulated plan can help stakeholders understand the need for, or even appreciate, the engagement, they are less likely to embrace the fieldwork process, itself. For example, a retail operations manager concerned about shrink may welcome the idea of a loss-prevention audit, but may be less enthusiastic about the auditor's requirement to conduct time-consuming inventories after hours. While auditors should avoid the temptation to eliminate or modify key audit procedures to appease stakeholders, they should try to reduce the audit burden by compiling their own documentation, such as running reports and queries, scheduling observations at mutually agreed-upon times, and being fully prepared at the onset of fieldwork to limit the audit duration.

ISSUE VETTED, QUANTIFIABLE, AND ACTIONABLE REPORTS

The audit report can be the most valuable product of an engagement, but

FOURLEAFOVER / SHUTTERSTOCK.COM

Thank You for Making **2018** a Success!

Through generous contributions from individuals, organizations, and IIA affiliates, the Internal Audit Foundation continues to develop groundbreaking research and educational resources to advance the profession.

Foundation Strategic Partners ($30,000+)

Crowe

protiviti®
Face the Future with Confidence

The Institute of Internal Auditors

The Institute of Internal Auditors Chicago Chapter

The Institute of Internal Auditors Dallas Chapter

The Institute of Internal Auditors Houston Chapter

Foundation Partners ($15,000 – $29,999)

Deloitte.

EY
Building a better working world

Grant Thornton

KPMG

**Larry Harrington,
CIA, QIAL, CRMA**

pwc

Gold Partners ($5,000 – $14,999)

ExxonMobil Corporation

IIA–Central Ohio Chapter

IIA–Detroit Chapter

IIA–Kansas City Chapter

IIA–New York Chapter

IIA–Philadelphia Chapter

IIA–San Francisco Chapter

IIA–Toronto Chapter

N.G. Shankar, CIA

Paul J. Sobel,
CIA, QIAL, CRMA

Raytheon

Silicon Valley Bank

Support Our Vision and Mission. Make Your Donation Today!
www.theiia.org/Foundation

INTERNAL AUDIT FOUNDATION™

2019-2207

40% of respondents say internal audit has a strong impact and influence within the organization—up from 28% in 2016—according to Deloitte's 2018 Global CAE survey.

it also can be the most controversial. According to Deloitte's 2018 Global CAE Research Survey, 24 percent of participants listed helping the business respond to prior internal audit recommendations as a key strategic priority. As audit reports can have a widespread audience, including executive leadership and the board, stakeholders can be highly sensitive to negative feedback and how it is presented. While some stakeholder defensiveness is inevitable, internal auditors can make the audit report less controversial by preparing it under a highly collaborative and iterative process. While stakeholders should not author, redact, or edit an audit report, they should be given the opportunity to review drafts and ask questions until consensus is achieved before publishing it to a larger audience.

Additionally, audit recommendations should not come in the form of mandates, but rather as value propositions supported by tangible, quantifiable benefits. For instance, an auditor completing a Lean Six Sigma assessment can advise stakeholders that implementation of the proposed recommendations could potentially drive productivity up X percent and reduce operating costs by Y percent. If such data is not available in house, the auditor can at least point to successful case studies, such as General Electric's savings of $12 billion in the first five years after implementing Six Sigma. Lastly, to the extent that supporting management in its implementation of audit recommendations does not impair independence, auditors should offer to lend support throughout the process to ensure the recommendations are timely and satisfactorily addressed.

CONVERT SOLICITED FEEDBACK INTO ACTION

While soliciting real-time, informal feedback throughout the engagement life cycle is valuable, internal auditors cannot underestimate the importance of formal, recurring feedback mechanisms such as stakeholder surveys and quality assessment interviews. According to KPMG's 2018 Benchmarking Survey, three-quarters of respondents use a formal stakeholder satisfaction questionnaire. While effective surveys can take several different forms, internal audit surveys should be anonymous to ensure candid feedback, and leave the respondents with the opportunity to provide free-form responses—in lieu of pure multiple choice or numerical rating scales—to expound upon improvement opportunities with examples and recommendations.

> Auditors can make the audit report less controversial by preparing it under a highly collaborative and iterative process.

While administering a survey can be seen as a gesture of good faith to the stakeholder, it can be perceived as mere lip service without being converted into visible actions. To ensure stakeholders realize their feedback is not in vain, CAEs should consider summarizing the survey results, including the improvement opportunities and subsequent action plans, and communicating them to impacted stakeholders via reporting or debrief meetings.

PERFORM QUALITY ASSESSMENTS

The most valuable feedback an internal audit function can receive is directly from its stakeholders. Nonetheless, the performance of periodic quality assessments, as mandated by The IIA's *International Standards for the Professional Practice of Internal Auditing*, can help identify additional opportunities to align with generally accepted best practices. While a quality self-assessment using IIA-provided tools is generally sufficient, CAEs must adhere to The IIA's guidance to engage an independent party at least once every five years to complete the assessment, and ensure stakeholders are apprised of this practice to avoid the perception of a conflict of interest. Similar to the audit feedback surveys, CAEs should consider reporting the results of their quality assessments, including any subsequent action plans, to impacted stakeholders to demonstrate the audit function's commitment to continuous improvement.

A CUSTOMIZED APPROACH

Internal audit functions face constant challenges juggling diverse and occasionally conflicting expectations from their stakeholders, including business-unit leads, executives, board members, external auditors, and regulators. Unfortunately, these challenges cannot be alleviated by a single action or even a one-size-fits-all approach. However, an effective internal audit function can navigate widespread stakeholder expectations through a multifaceted approach that engages stakeholders in every aspect of the engagement life cycle. By differentiating effective stakeholder management from constantly trying to please everyone, internal auditors can avoid the fate of Aesop's Miller and His Son. Ia

JACK PELIKAN, CPA, CISA, CISSP, *is senior director of internal audit at Caleres Inc. in St. Louis.*

Board Perspectives

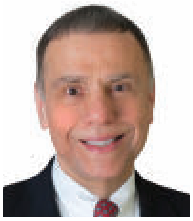
BY MATT KELLY

A BOARD'S-EYE VIEW OF DIGITAL DISRUPTION

Organizations fear keeping up with born-digital competitors.

ERIC ALLEGAKOEN

TOM RICHLOVSKY


ALAN SIEGFRIED

At the end of every year, North Carolina State University and Protiviti publish a survey report on the enterprise risks occupying the minds of board directors and corporate executives for the following year. The Executive Perspectives on Top Risks report is always worth reading, and the 2019 edition does not disappoint.

What's topping the charts for this year's risks? Fear that the organization's existing operations and technology won't match performance expectations, especially against "born digital" competitors. That's no surprise. Taxis vs. Uber, hotels vs. Airbnb, broker dealers vs. robo-advisors—even the record industry vs. iTunes, a bit further back in history. Fear of more nimble, next-generation competitors, while your own organization is too hide-bound to get out of its own way, is not new.

So how should boards approach digital transformation? "It's something we talk about all the time," says Tom Richlovsky, audit committee chair of United Community Banks (UCB), a regional bank based in Georgia. A generation ago, UCB would never find itself squeezed by fintech startups or global banks courting everyone with a mobile phone. Today, UCB does. As Richlovsky says: "We have a front-row seat to how digital disruption operates."

The Strategic Threat

First, let's appreciate what happens with digital disruption. Born-digital firms can be so disruptive because they build business models for existing problems with dramatically less commitment to physical assets. That's the economics of it.

What happens operationally is a bit more nuanced. Digital firms can be more nimble because they are less bound to specific ways of doing things. Code is code, after all; if you don't like how it works, you can change it.

So digital firms are less committed to physical assets, and they can pick off specific problems in a business, introducing whatever new solution they want. That's how they disrupt the business models of established companies. They provide new choices to customers, who often depart the organization's model for the upstart's.

A big part of success at digital transformation, then, involves close observation of the organization's customers, plus a big dollop of imagination about what new relationships the organization can forge with them. "You have to understand what's happening with your customers so that you can get a step ahead of them, and get them to adopt technologies and become a better customer who stays with you," says Glenn Gow, a former board director at data analytics firm acuteIQ, who now advises boards on digital strategy.

Gow uses the example of ordering pizza. In the last

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

TOP RISKS FOR 2019

1. Existing operations meeting performance expectations, competing against "born-digital" firms.
2. Succession challenges and ability to attract and retain top talent.
3. Regulatory changes and regulatory scrutiny.
4. Cyber threats.
5. Resistence to change operations.
6. Rapid speed of disruptive innovations and new technologies.
7. Privacy/identity management and information security.
8. Inability to use analytics and big data.
9. Organization's culture may not sufficiently encourage timely identification and escalation of risk issues.
10. Sustaining customer loyalty and retention.

Source: Executive Perspectives on Top Risks 2019, Protiviti and North Carolina State University Poole College of Management's ERM Initiative

decade, consumers have moved from placing orders by phone to placing them by app. Online ordering eases the transaction for the customer and generates more customer data for the pizza company—a great example, Gow says, of digital disruption benefitting all parties involved.

Too many boards fear the threats of digital disruption more than they embrace its opportunities. The truth is digital disruption will drive both threats and opportunities. "The ways in which disruption can occur are multiplying," Richlovsky says, so the board needs to educate itself on all those ways.

Governance of Digital Disruption

In theory, if the board wants to gain more knowledge about the risks a certain issue might pose, step 1 is to ask the internal audit function. Digital disruption, however, poses so many strategic questions that it doesn't lend itself to such straightforward analysis. It's an open question whether most audit functions could understand and assess the challenges at hand.

"The concept is a good idea," says Alan Siegfried, who is on a bank's audit committee now and has served on the audit committees of UNICEF and Bon Secours Health System, "but realistically, probably 90 percent of the audit functions out there don't have the qualifications or skill sets to do that well."

Boards can take a few steps to improve that picture. First, they can identify strategic priorities for digital transformation more clearly, so the business units can determine which operations and business processes should be digitally transformed, and how. For example, should the business focus more on the "offense" of developing new products or services, or the "defense" of developing improvements to existing ones? Should it cut fixed costs by moving to cloud-based services, even if that drives up security, privacy, and litigation risks?

Gow suggests that boards work closely with the CEO and the chief information officer (CIO) on those points. After all, if success at digital disruption depends on astute data analytics and bold imagination on how to serve the customer in new ways—the CIO handles the former, the CEO the latter.

Then the board and management can develop a technology strategy that supports digital transformation, including the critical step of what new controls will be necessary to implement the strategy. For example, moving business processes to the cloud and taking advantage of mobile devices, so the organization can launch an international sales force with more in-the-field agents, is a reasonable digital transformation goal.

The technology strategy, however, will raise questions such as: How can the company harness all its operational data, if the data is stored within different apps? How does the company secure its data on employees' personal devices? At that point, internal audit or compliance functions can return to the conversation, because the digital transformation goal is already laid out. The questions are more about risk management to ensure the transformation doesn't go awry.

Oversight of Digital Transformation

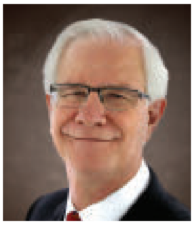
So, which board committee should have digital transformation as part of its remit? A strong argument exists that *no* specific committee should own it. The only logical candidates would be the audit committee or a risk committee, and they are, to use Richlovsky's phrase, "reactive committees." That is, they seek to ensure that safeguards are in place for whatever strategies the organization pursues. How an organization moves into the digital world, however, is a strategic choice unto itself. Thus, the whole board should be responsible for infusing digital awareness into every organizational strategy and objective.

"When it's a strategic journey the company is going through, it needs to be a full board topic," says Eric Allegakoen, head of internal audit at Adobe and chair of The IIA's Audit Committee. "Once the strategy becomes clear in how it's getting executed, there would be responsibilities at the audit committee or risk committee level to monitor progress."

Indeed. And if the risks listed by Protiviti (see "Top Risk for 2019," this page) are any indicator, digital transformation will likely permeate boardroom conversations for some time.

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

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



BY J. MICHAEL JACKA

YOU CAN ALWAYS TURN AROUND

If the work you're performing doesn't have a reasonable purpose, just say no.

During an audit, you discover a department's most significant project was misguided, no longer aligned with organizational needs, and a waste of the department's limited resources. Everyone involved agrees with your assessment, leading to the question, "Why continue?" Leadership responds with reasons such as: "We always complete every project," "We just do as we're told," and "We can't stop—it would be an admission that we failed." What do you do?

Any auditor worth his or her completed time sheet would recommend that management adjust, modify, or stop the project dead in its tracks, allowing the department to get to work on something (anything) more important. Unfortunately, while we might do an excellent job of telling others what to do, many audit departments do not practice what they preach and often move forward on potentially inconsequential projects as though there were no turning back.

Stories from the real audit world—experiences from my own career or that I learned about from others firsthand—help illustrate this problem. Details have been removed to protect the innocent, the guilty, and the somewhere-in-between.

- While providing support for the external auditors, the chief audit executive (CAE) explained that one of the planned tests did not apply to the way the company operated. The accountant agreed but explained the test would have to be completed because "it was a requirement of the audit program."
- Although auditors were told the audit schedule was flexible, no one ever deviated from it. The audit leader would say, "If we went to the audit committee and asked for a change, they would think we didn't know what we were doing when we first put the plan together."

Unfortunately, it wasn't too hard for me to produce these examples—a sign that the practice of continuing to do work obstinately just because it is "in the plan" continues to haunt our profession. We claim we want to be agile, but we don't even have the agility necessary to adapt to changing circumstances.

There is nothing—no project, no audit engagement, no plan—that internal audit should require itself to complete just because it has already been started, it is what has always been done, or the more dreaded, "we don't want to have to explain why we changed." This is not value, this is not service, this is not professionalism—this is blind adherence to meaningless dogma.

Look ahead at the work you are doing and, if it has no reason—if the risk isn't there, if the requirements aren't there, if it is done to support a promise that makes no sense—just say no. Turn around and start something new, different, and better. Ia

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

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

A MATTER OF PRIVACY

Internal auditors can assess data privacy governance within their organizations.

MIKE MAALI
Internal Audit,
Compliance,
& Risk Management
Solutions Leader
PwC US

PAM HRUBEY
Managing Director,
Risk Consulting
Crowe

How do regulations like GDPR address issues with protecting personal data?

MAALI Europe's General Data Protection Regulation [GDPR] pushes companies doing business with Europeans' data to do three things well: give people control over their data, respond quickly to breaches, and embed privacy controls throughout their business. The law has changed the privacy function from a paper-based exercise of policies and contracts to a business-transformation program affecting every product and service that uses European data.

HRUBEY GDPR and regulations like the California Consumer Privacy Act, Brazil's new General Data Protection Law, and new and revised regulations in Australia, China, and Japan highlight the need for companies to get their data protection practices in order. Organizations tend to have common challenges relating to data protection, including difficulty maintaining a current inventory of personal data, failing to connect privacy notices and privacy consents to personal data, and keeping personal data longer than is necessary to complete the business purpose described. Companies also are challenged with maintaining the accuracy of personal data and responding timely to data subject access requests.

What are the consequences of failing to comply with data privacy regulations?

HRUBEY Under GDPR, fines for a failure to comply—particularly with data subject consent-related requirements—can be up to €20 million ($22.5 million), or 4 percent of the organization's global annual turnover, whichever is larger. Organizations that have a data breach-related violation can be fined up to €10 million ($11.2 million), or 2 percent of the organization's global annual turnover, whichever is larger. Operationally, regulators also can elect to stop the flow of personal data out of the European Union (EU), unless data is going to a country deemed to have adequate data protection provisions under EU regulations—the U.S., for example, does not have that designation. Regulators also can restrict an organization's ability to use the personal data of EU residents until remediation is made of the underlying compliance problems. And perhaps more problematic is the damage to the organization's reputation. In a highly digitized economy, customers must be able to trust organizations with their personal data.

MAALI A lot has been said about the maximum fine for an egregious violation of GDPR. But GDPR also gives European citizens a private right of action to bring lawsuits against companies for privacy violations, and courts have no limit to the penalties and awards they approve.

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

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

Perhaps the biggest risk is if a regulator imposes an injunction to prevent a company from continuing to process EU personal data. This could stop a product or service overnight.

How can organizations demonstrate that they are safeguarding information?

MAALI The most visible way for companies to demonstrate a high level of data-privacy maturity is to offer employees and consumers a portal where they can view, correct, and delete their data and express opt-in and opt-out privacy consents. In addition, a well-documented process for assessing, monitoring, and mitigating risk can provide confidence to key stakeholders.

HRUBEY Regulators expect organizations to be able to defend the risk-based decisions they have made regarding implementation of GDPR's requirements. On the customer side, organizations should be transparent about the safeguards they are using to protect personal data. Privacy notices should, using plain language, include a description of how the organization protects the personal data under its care and be updated when the organization adjusts the safeguards used. Organizations should take a similar approach to privacy consent language, and take care to not process personal data before obtaining the data subject's consent. Organizations also should consider including information about their privacy program on their website.

What is audit's role in assessing privacy governance?

HRUBEY GDPR requires organizations to periodically assess compliance against the requirements. Internal audit generally is in an excellent position to make this assessment on behalf of the organization. The key to a successful privacy audit is to understand the organization's privacy landscape and the potential risks it faces. Mindful of those risks, internal audit can leverage existing audit methodologies and follow standard internal audit methodology to understand the organization's performance in those potential risk areas. Privacy is ever-changing, so being agile regarding the risk landscape is the best approach to the privacy audit. Privacy team members along with their legal support colleagues are responsible for determining how regulations like GDPR apply to the organization, and then ensuring that appropriate program materials are prepared. Internal audit can assess whether the organization has pulled through the policies and procedures as expected.

MAALI Internal audit can play a range of roles helping a company accelerate its privacy journey. The first is to consider data privacy as a material risk for the organization to monitor. Internal audit also can advise management on the selection of a privacy control framework that is most applicable to the company's industry. It can assess and report the company's status against that framework, and make recommendations on which stakeholders in each line of defense are best positioned to own the remediation of the control gaps. Internal audit also is positioned to test these controls on an ongoing basis, including reporting progress to senior management and the board.

What should internal audit assess regarding third-party data privacy compliance?

MAALI Internal audit can help the organization reduce third-party privacy risk in several ways. First, internal audit can ensure that management has sufficient processes to identify high-risk suppliers and perform ongoing monitoring. In addition, internal audit can ensure that sufficient protections exist within third-party contracts, including right to audit provisions. Finally, internal audit can play an important role in assessing the data privacy controls for high-risk suppliers.

HRUBEY Under GDPR, third parties who are processing personal data on behalf of an organization are accountable for complying with the related regulatory requirements. This does not mean that the organization hiring a third party is off the hook. Because the hiring organization is usually operating as a controller under GDPR—the entity that determines the purposes, conditions, and means of the processing of personal data—the controller may still have liability if the instructions provided to the third party regarding processing personal data were inappropriate. Organizations should have contracts that address expectations associated with privacy and data protection. Internal audit can evaluate contract compliance.

What controls are most needed to ensure the organization complies with data privacy regulations?

HRUBEY The answer depends, at least in part, on the organization's work, its industry, and the specific personal data it processes. Generally, organizations need data privacy-related controls, including an individual responsible for determining what regulations apply and what the organization must do to comply; risk assessment processes that can pinpoint privacy and data protection-related risks; clear policies and procedures for employees to follow; periodic training; and investigations into noncompliance that identify associated root causes. Strong information security-related processes should include, for example, access controls by role and, where appropriate, by individual; encryption of electronic equipment, including laptops and mobile devices; physical security; and logical security.

MAALI The most difficult, but foundational and important privacy control, is to maintain a current inventory of all personal data, both within the organization and among relevant third parties. All lines of defense will have a role in meeting that objective. With a sustainable and accurate data inventory, companies can deploy other controls around information security and data-subject rights. Ia

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

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

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

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

SEPT. 13–15
Internal Audit Student Exchange
Rosen Centre
Orlando, FL

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

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

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

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

IIA TRAINING

www.theiia.org/training

NEW Auditing IT Governance
OnDemand

NEW Understanding and Auditing Big Data
OnDemand

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

APRIL 8–17
Root Cause Analysis for Internal Auditors
Online

APRIL 9–12
Multiple Courses
New York

APRIL 15–18
Statistical Sampling for Internal Auditors
Online

APRIL 16–25
NEW Advanced Risk-based Auditing
Online

APRIL 22–24
COSO Internal Control Certificate
Tampa, FL

APRIL 22–MAY 1
Cybersecurity Auditing in an Unsecure World
Online

APRIL 30–MAY 3
Multiple Courses
Seattle

APRIL 30–MAY 9
NEW Fundamentals of Risk-based Auditing
Online

MAY 6–15
Audit Report Writing
Online

MAY 7–10
Tools & Techniques III: Audit Manager
Houston

MAY 7–10
Multiple Courses
Boston

MAY 7–10
Multiple Courses
Washington, DC

MAY 7–16
Fundamentals of IT Auditing
Online

MAY 8–9
Data Analysis for Internal Auditors
Online

MAY 13–22
The Effective Auditor: Understanding and Using Emotional Intelligence
Online

MAY 14–17
Tools & Techniques I: New Internal Auditor
Salt Lake City

MAY 14–17
Multiple Courses
Chicago

MAY 21–23
COSO Internal Control Certificate
Minneapolis, MN

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 stephen.zwelling@theiia.org

BY STEPHEN N. ZWELLING

REDEFINING INTERNAL AUDITING

The time has come to revisit how the profession defines itself.

While it has served the profession well for the last two decades, the definition of internal auditing needs an update. The current definition states: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." In many ways this description fails to provide management and stakeholders with an accurate picture of the profession, lacking clarity in several important areas.

First, internal auditing is a service, not an activity—the word *activity* diminishes its purpose and focus. Playing baseball is an activity. Cutting the grass is an activity. Service is what we do for the good of others. It is a higher calling than an activity and connotes greater importance.

When internal auditors perform their services, they inherently add value and bring about improvements—otherwise they shouldn't be in the organization. Saying the profession is "*designed* to add value and improve an organization's operations" implies the possibility of not achieving these aims. Internal auditors add value whenever they do their job correctly, even if the organization does not accept their recommendations.

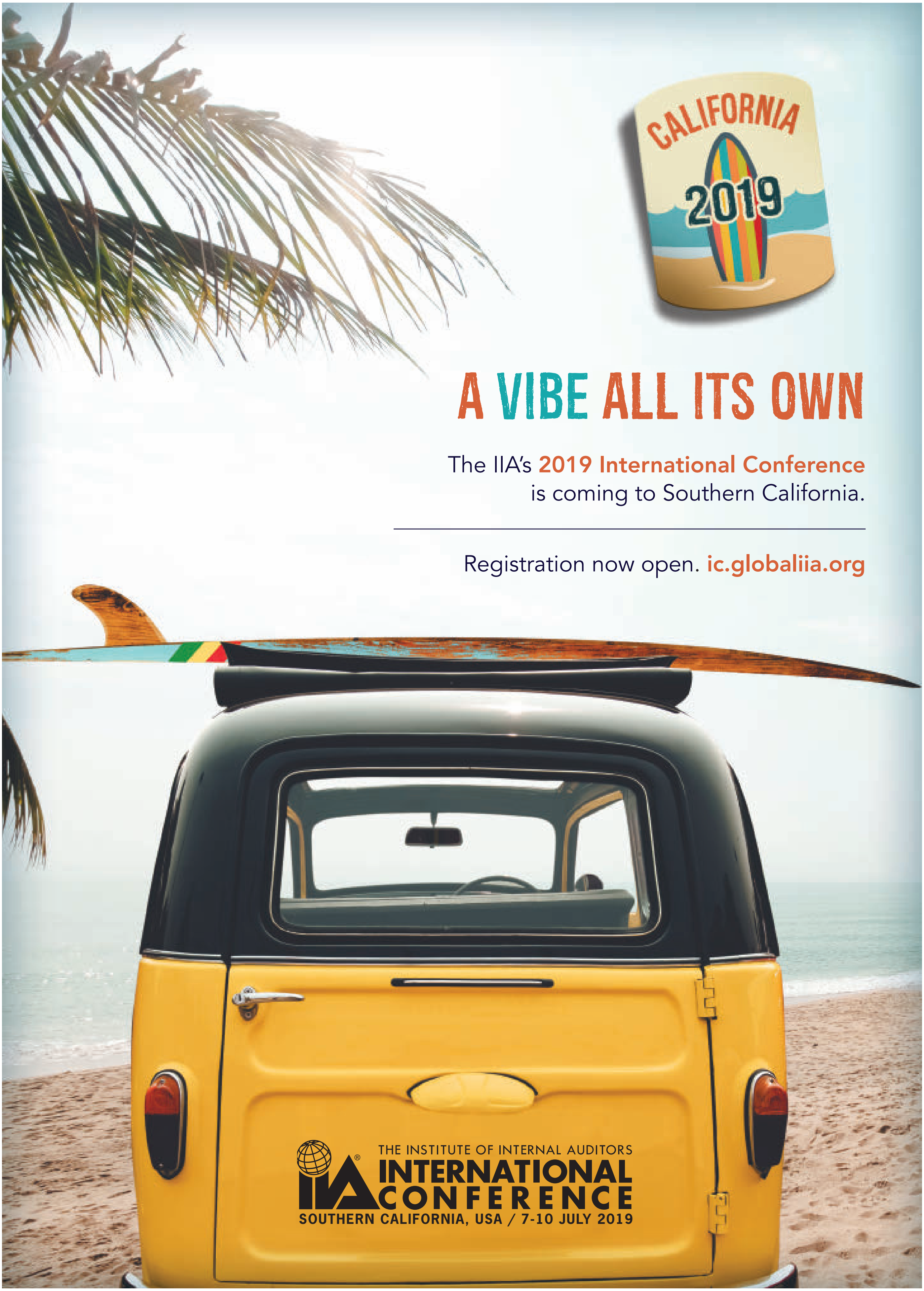
Moreover, auditors shouldn't need to specify a detachment from the organization for all types of engagements. Independence and objectivity are necessary for audit services, but not for consulting services. Consulting clients determine the scope of consulting services. Hence, objectivity and independence for these types of engagements do not present a problem—instead, competence is the key.

Lastly, the definition makes no reference to the importance of internal audit as an *internal* function. Organizational change can significantly affect the systems and controls that auditors help management assess. Change and its effects should be reviewed proactively, before implementation. If the organization does not maintain an audit presence internally, the chances for proactive review decline significantly and the associated risks increase significantly. Internal audit's relationships with clients, fostered by in-person interactions, are essential to ensuring practitioners are called upon when the organization contemplates change.

With these considerations in mind, I propose a revised and expanded definition: "Internal auditing is a service that performs both auditing and consulting work to add value and improve the organization's operations. It accomplishes these objectives using a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Internal audit works closely with the individuals it services to build long-term relationships so together, change is reviewed proactively for the good of the organization." I hope this revision will mark the beginning of a dialogue on how our profession should be defined. Ia

STEPHEN N. ZWELLING, CIA, CPA, CISA, *is owner of KISS in Lewis Center, Ohio.*

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


CALIFORNIA
2019