Ia
INTERNAL AUDITOR

DECEMBER 2019

A PUBLICATION OF THE IIA

A Framework for AI Audits

Be Brave Auditors

Using Bots to Enhance Assurance Capabilities

Thinking About How You Think

RISKS IN VIEW

Internal audit must be resilient and outspoken in pressing the organization to act on threats on the horizon.

A New Look
at Internal Auditing.

Ia
INTERNAL AUDITOR

DECEMBER 2019 VOLUME LXXVI: VI

FEATURES

Featuring

Internal Auditor Blogs

Voices with viewpoints on the profession

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

Chambers on the Profession:
Seasoned Reflections on Relevant Issues

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

Solutions by Soileau:
Advice for Daily Audit Challenges

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

READ ALL OF OUR BLOGS. Visit InternalAuditor.org.

Ia
INTERNAL AUDITOR

Ia
INTERNAL AUDITOR

DECEMBER 2019 VOLUME LXXVI: VI

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Audit Wellness There's much more to auditing than skills and knowledge – how auditors treat themselves day to day impacts their effectiveness as practitioners.

Bots for Small Shops Even when challenged by limited resources, auditors should not assume robotic process automation is out of reach.

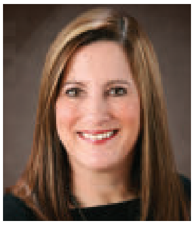
The Analytics Journey The road to implementing data analytics begins with defining the elements of a program.

Special Delivery Contract fraud is indicated when several trucking companies bribe a senior employee at a delivery firm in a scheme to land lucrative deals.

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: PHOTO ILLUSTRATION BY SEAN YATES (PHOTOS, LEUNGCHOPAN, ANTHONY BOLAN, LJUPCO SMOKOVSKI / SHUTTERSTOCK.COM); THIS PAGE, TOP: DNY59 / ISTOCKPHOTO.COM, BOTTOM: ZAKOKOR / ISTOCKPHOTO.COM



ON PACE WITH TECHNOLOGY

The accelerating pace of technology advancements is creating significant disruption within organizations—and it appears internal auditors may not be keeping pace. A new report from The IIA, OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk, reveals that one risk area in which internal audit may be falling behind is data and new technology.

According to OnRisk, only 17% of internal auditors consider themselves knowledgeable about data and new technology, lower than the 42% of board members and 26% of those from the C-suite who consider themselves the same. For auditors to be taken seriously in the boardroom, they must address these knowledge gaps.

The OnRisk report recommends that chief audit executives "dedicate resources to better understanding how the organization is leveraging data and technology in new ways." Internal audit should be able to provide assurance on the impact of data and new technology on the "collection, management, and protection of data," the report says.

To do that, internal auditors need to ensure they're educating themselves in these areas. In that vein, auditors may want to read "Framing AI Audits" (page 29), which takes an in-depth look at internal audit's role in assessing artificial intelligence risks and testing system controls. Also in this issue, "Bots of Assurance" (page 42) considers how audit functions can catch up with their organizations' use of robotic process automation by deploying bots to enhance their assurance capabilities. Finally, readers may want to check out the first of a three-part series of reports coming from Deloitte and the Internal Audit Foundation on new technologies, Moving Internal Audit Deeper Into the Digital Age: Part 1 (http://bit.ly/DigitalAgePart1).

According to OnRisk, as risks around data and new technology grow in relevance over the next five years, risk management players need to build knowledge in this area. Internal audit professionals who take their fate into their own hands and improve their tech knowledge will likely find themselves in high demand, as OnRisk also notes organizations are struggling to attract and retain talent with data and IT skills.

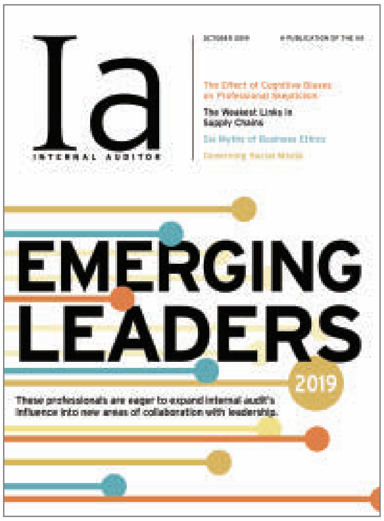
Finally, with this issue we say goodbye to our designer, Joe Yacinski. I have worked with Joe since I joined The IIA in late 2000, and I will greatly miss our collaborations. His thoughtful and creative approaches to the many challenging articles we've brought him over the years—how does one illustrate internal control?—have resulted in the magazine receiving numerous accolades. Joe's contributions have helped make the magazine the professional publication it is today. Joe, thank you, and we wish you well.

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.


OCTOBER 2019
A PUBLICATION OF THE IIA
Ia
INTERNAL AUDITOR
The Effect of Cognitive Biases on Professional Skepticism
The Weakest Links in Supply Chains
Six Myths of Business Ethics
EMERGING LEADERS
2019
These professionals are eager to expand internal audit's influence into new areas of collaboration with leadership.

Internal Audit Skills

I suppose the main challenge will be to transform matured internal audit staff competencies that lie mostly within financial education and backgrounds to such things as SQL and Python.

PAVEL VOLKHIN *comments on Seyyed Mohsen Hashemi's "Top Challenges of Automating Audit" (October 2019) on LinkedIn.*

Audit Survey Reviews

Far too many surveys include poorly worded questions. A critical step in preparing a survey is to have it reviewed by an independent party. This can help ensure the phrasing is not misleading. Another important consideration is to have the survey piloted by a small group first to see what responses are given. Both of these thoughts are suggested by Jim, but without the emphasis I think they deserve. A bad question or two can drastically skew the results of a survey.

RICHARD FOWLER *comments on James Roth's online series, "Auditing Culture: Audit Project Surveys" (InternalAuditor.org).*

Changing Assumptions

I absolutely agree with this, but as a profession we have to get better at demonstrating the skills we have. We can't change assumptions without our own efforts.

DAVID HILL *comments on Neil Hodge's "A Limited View" (InternalAuditor.org) on LinkedIn.*

Social Engineering Controls

The low-tech solution for voice and video orders is to require a passphrase that includes at least eight alphanumeric characters (both letters and numbers). And it should be changed periodically. Employees need to be fully aware of the requirements and that there are no exceptions, ever. And the executives need to be the ones communicating that policy personally to key employees who process or can order payments or transfers.

PHIL CASKANETTE *comments on Art Stewart's "Deepfake Deception" (InternalAuditor.org).*

Who Is at Fault?

The question points to all key pillars of governance. Who is at fault carries a strong message to all. Did everyone play their part? What happened to oversight and assurance from management and audit? We are all responsible if no one came out boldly and shouted it. Internal auditors are usually expected to red flag some of these issues formally or informally and must have evidence to exonerate themselves from any blame or answering the question, "What did you do?"

GODFREY KILENGA *comments on the Chambers on the Profession blog post, "When Boards Are Surprised, Who's at Fault?" (InternalAuditor.org).*

Ia
INTERNAL AUDITOR
DECEMBER 2019
VOLUME LXXVI:VI

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
Rick Wright, CIA

IIA PRESIDENT AND CEO
Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA

IIA CHAIRMAN OF THE BOARD
J. Michael Joyce, Jr., CIA, CPA, CRMA

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

ADVERTISING
sales@theiia.org
+1-407-937-1388; 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")

An Exclusive
Opportunity

Security, governance, top IT concerns... Workers want gender equality audits... How boards prepare for downturns... Fraud fighters needed as losses rise.

Update

NO SEAT AT THE TABLE FOR IT SECURITY

Most security functions lack access to the board and senior management.

40% do not report to the board at all.

14% only report to the board following a security incident.

28% say the board and CEO determine and approve the organization's acceptable level of cyber risk.

21% say the board and CEO require cybersecurity due diligence in the merger and acquisition process.

Source: AttackIQ and Ponemon Institute, The Cybersecurity Illusion: Enterprise Security Remains Reactive

EXECUTIVES FOCUS ON THE ECONOMY

Fiscal crises are among business leaders' top concerns.

Economic-related issues lead business executives' concerns worldwide, according to the World Economic Forum's (WEF's) Regional Risks for Doing Business 2019 report. The survey of nearly 13,000 business leaders across more than 130 countries identified fiscal crises as the greatest risk to businesses globally.

Two other top risks also were economic in nature, with unemployment or underemployment ranking third and energy price shock coming in fourth. The survey also notes those two risks' links to social disruption, tying them to failure of national governance and profound social instability—ranked fifth and sixth, respectively. Respondents identified cyberattacks as their second biggest challenge.

"At a time when global economic growth appears fragile, business leaders are deeply concerned by their governments' fiscal resilience," says Emilio Granados-Franco, head of Global Risks and Geopolitical Agenda at the Geneva-based WEF.

The report also cites region-specific findings, noting that environmental risks were the top concern in South Asia and East Asia/the Pacific. Moreover, profound social instability and interstate conflict rank highest in Eurasia, while the top risks in North America centered on digital asset vulnerabilities.

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

IMAGES: TOP, DNY59 / ISTOCK.COM; LEFT, LEBENDIGGER / SHUTTERSTOCK.COM

Meanwhile, failure of national governance tops the list for Latin America. In the Middle East and North Africa, survey participants are most concerned with energy price shock. And in sub-Saharan Africa, respondents say they are most concerned about the inability of their economies to create jobs.

The WEF points to the need for an integrated approach to addressing risks. "Only by addressing economic risks and societal, technological, and environmental risks in an integrated manner, can stakeholders truly build resiliency," Granados-Franco says. **— D. SALIERNO**

SECURITY AND GOVERNANCE TOP IT AUDIT CONCERNS

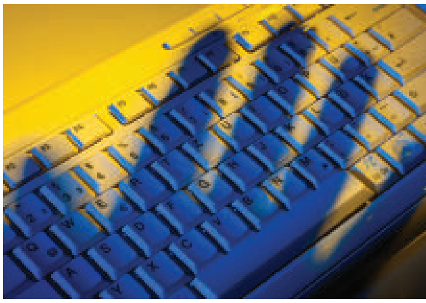
Audit professionals rank their departments' greatest technology challenges.

Auditors rank "IT security and privacy/cybersecurity" and "data management and governance" as their top two technology challenges, according to a recent survey. The 2019 Global IT Audit Benchmarking Study, conducted by ISACA and Protiviti Inc., polled more than 2,200 chief audit executives, internal audit professionals, and IT audit vice presidents and directors worldwide.

Data management and governance jumped significantly to its second place ranking, ranked at No. 10 last year. The researchers note that, as organizations seek to leverage data with robotic process automation and artificial intelligence, IT audit functions are focusing more on evaluating risks related to data collection and reporting.

Respondents identify emerging technology and infrastructure changes, staffing and skills challenges, and third-party/vendor management, respectively, as their remaining top five challenges.

Researchers also point to the importance of internal audit's partnership with the IT function in the area of risk management. "As these two groups work together," says ISACA Technical Research Manager Robin Lyons, "risk management becomes a shared, real-time effort that reduces guesswork by IT audit as to which project challenges and risks truly exist." **— D. SALIERNO**



THE AVERAGE OVERALL COST OF FRAUD IS

1.75%

of revenues in Indonesia, Malaysia, the Philippines, and Singapore.

OVERALL COSTS OF FRAUDULENT TRANSACTIONS IN THE REGION ARE

350%

more than the actual value lost from those transactions.

"The digital space is where the battle against fraud is heating up, with our report highlighting identity verification as a key challenge," says Alisdair Faulkner, chief identity officer, Business Services, at LexisNexis Risk Solutions.

Source: LexisNexis Risk Solutions, 2019 True Cost of Fraud Asia-Pacific study

WHEN ALL IS NOT EQUAL

Gender equality audits should be mandatory, a new survey says.

Two-thirds of workers worldwide say gender equality in the workplace is achieved when men and women are paid the same, according to research commissioned by MAXIS Global Benefits Network. But as the United Nations has stated, equality goes beyond equal pay. It means women have equal opportunities for leadership and a work environment free from sexual harassment and discrimination.

"Pay parity is part of a wider discussion about the workplace, which includes employee benefits packages and workplace culture,"

IMAGES: TOP, LISA S. / SHUTTERSTOCK.COM; RIGHT, PROSTOCK-STUDIO / SHUTTERSTOCK.COM

ONRISK
A GUIDE TO UNDERSTANDING, ALIGNING, AND OPTIMIZING RISK
2020

MORE VISIT http://bit.ly/DottyHayes to read an extended interview with Dotty Hayes.

says Patsy Langridge, global director of marketing and communications for London-based MAXIS. The survey polled 1,000 office workers in 10 different countries.

A sign of this concern is that two-thirds of respondents say organizations should be required to conduct an annual gender equality audit "to see how their workplace is evolving," Langridge points out. Such audits check the institutionalization of gender equality in organizations and identify aspects of organizational culture that may discriminate against one gender. Gender equality audits aren't common, though, with only 27% reporting that their organization performs them.

Still, pay gaps are an obvious example of gender disparity in the workplace. One practice that may help address these gaps is performing pay equity audits, according to a report, Navigating the Growing Pay Equity Movement. Pay equity audits are driven largely by increasing pay equity regulations, notes the report from Harvard Business Review Analytic Services and Trusaic, a software and services company based in Los Angeles.

The survey of 589 senior executives finds that the U.S. is playing catch-up to the U.K. Eighty-six percent of U.K. respondents say their organization has conducted a pay equity audit versus 77% in the U.S.
– S. STEFFEE

RECESSION RESILIENT

Facing an economic downturn, organizations need escape hatches, says Dotty Hayes, a board member in Silicon Valley and former CAE.

How do boards evaluate the risk and potential impact of a recession – and how can internal audit help? I do my own environmental scanning such as staying current with news sources and updates from professional organizations. I also look for management's viewpoint on the economy and risks to the business, specifically. In budgeting or forecasting discussions, I expect a dialogue on the range of potential outcomes and am attuned to the risk attitude taken by management. Are they barreling ahead without regard to what is happening in the world? Are they afraid of the dark? Neither extreme is good. In particular, I look for ways in which business plans provide optionality – the quality of being chosen but not obligatory – and escape hatches to increase resilience in the face of uncertainty.

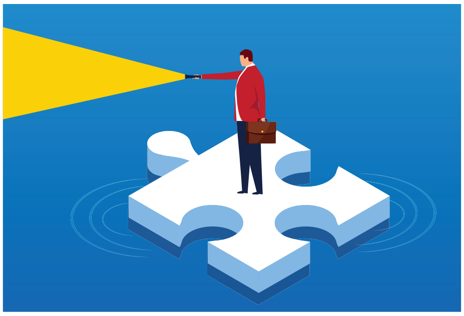
Internal audit also should be doing environmental scanning as part of its risk assessment processes. As auditors are on the ground with local management teams and having discussions deep within the organization, they may pick up signals before they make their way up the management chain. Developing a process for collecting and communicating this information in a way that is helpful to senior management, but doesn't leave local management feeling exposed, is critical to success.

FEW INVESTIGATORS ON THE CASE

Organizations limited in stopping fraud losses, ACFE says.

Nearly half of in-house fraud investigators say their organizations are more vulnerable to external fraud than they were two years ago, the Association of Certified Fraud Examiners (ACFE) reports. About eight in 10 respondents say their organizations recover 50% or less of fraud losses, the 2019 In-House Fraud Investigations Team Benchmarking Report notes. Fifteen percent don't recover any.

Contributing to the problem, more than half of surveyed organizations don't adequately staff their anti-fraud teams, say the 886 ACFE-member fraud investigators who responded to the survey. The typical in-house investigator closes 39 cases annually.



"Without adequate resources or staff, fraud examiners are limited to how much they are able to sufficiently investigate and stop fraud," says Bruce Dorris, president and CEO of Austin, Texas-based ACFE.

Most respondents say management in their organization adequately understands fraud risk, and most expect investments in anti-fraud programs to increase in the next two years. **– T. MCCOLLUM**

PHOTO: RIGHT, Z_WEI / ISTOCK.COM

BY MAJA MILOSAVLJEVIC EDITED BY JAMES ROTH + WADE CASSELS

THE LINES OF INDEPENDENCE

Several proactive steps can help internal auditors deal with challenging ethical situations while keeping their independence intact.

A lead auditor comes to work one day and is instructed to do an audit engagement with another auditor. However, the lead auditor is aware that the indicated team member is not independent with regard to the underlying audit subject. The prudent and diligent lead auditor presents this information to the relevant superior and asks that the team member be replaced. Yet, not only is the compromised auditor left on the engagement, but the lead auditor is then instructed not to share this information with anyone and to conduct the audit engagement as initially planned. What should the lead auditor do?

Standard 1100: Independence and Objectivity says internal auditors are expected to be objective and independent in performing their professional duties. However, there isn't always specific guidance on how they should behave in situations that put ethical pressure on them. The first question is whether the auditor is even able to recognize such a situation. Once that is determined, the next relevant question is who can the auditor escalate the issue to. In such instances, the auditor may be afraid of losing his or her job by speaking up about these kinds of issues.

Several suggestions may help internal auditors deal with challenging ethical situations while protecting their own independence.

Start From the Beginning

Internal auditors are obligated to adhere to The IIA's Code of Ethics, the principles and expectations that govern the behavior of auditors in conducting their work. The Code of Ethics comprises integrity, objectivity, confidentiality, and competency. Although these principles are general in their nature, each has minimum requirements for conduct and behavioral expectations. Ultimately, they set the tone for the ethical practice of internal auditing. Thus, understanding and keeping in mind the requirements outlined in the Code of Ethics is an excellent starting point for every internal auditor in preserving his or her independence and conducting ethical audit engagements (see The IIA's implementation guidance on the Code of Ethics released in early 2019).

Speak Up

Presenting the situation realistically, based on facts, and with all the relevant details, can help auditors protect themselves. Internal auditors derive objective conclusions based on facts in their everyday work. By not speaking up, auditors can inadvertently become collaborators and supporters of ethical violations, which can impair their own

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

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

independence. Regardless of the specific circumstances, auditors should be aware that working on an engagement with another auditor whose independence is impaired weakens the independence of all involved auditors and the entire audit engagement.

Ask for Advice

Some ethical problems may not have an obvious solution. One good option may be to ask colleagues with more experience for advice. Without necessarily presenting the underlying situation with complete details, auditors can get valuable advice on how to protect themselves and create a win-win situation for everyone involved. Additionally, auditors might find it useful for their own professional development to listen to the experiences of their colleagues. Hearing about ethical challenges that others have faced can help auditors recognize the indicators of independence impairment.

Create Ethical Safeguards

There are no rules that can help auditors preserve their independence in every situation they may encounter while doing their jobs. Being unaware of their impaired independence does not excuse auditors from responsibility. On the contrary, it is up to all auditors to recognize the situation they are in and to adequately protect themselves. With the right approach to engagements, auditors can eliminate the possibility of compromising their independence.

> One effective way to deal with an ethical dilemma is to escalate the issue.

Some examples of situations that may adversely affect auditor independence include:

- Intimidation by management that makes the auditor concerned about his or her job.
- Personal relationships outside of the office with the CEO, chief financial officer, senior managers, chief audit executive (CAE), other auditors, or employees in the area being audited.
- Accepting gifts or favors from co-workers who may expect something in return.
- Assigning auditors to assurance engagements in their previous employment area less than one year after transitioning into internal audit.
- Expecting auditors to make business decisions and perform nonaudit-related operational tasks.
- Basing auditor compensation on the number of audit findings during engagements.

Escalate the Issue

One effective way to deal with an ethical dilemma in which there is a threat to an auditor's independence is to escalate the issue. In the case of the lead auditor letting the audit supervisor know of a compromised team member and the supervisor keeping that auditor on the engagement, the lead auditor should ask the supervisor why he or she wants to move forward with that auditor. If there is good reason, the lead auditor should remind the supervisor that the *International Standards for the Professional Practice of Internal Auditing* requires that the impairment be disclosed to relevant parties. If escalating the issue to the direct supervisor does not help, the next step should be to escalate it within the audit department. If the CAE then does not address the issue, the lead auditor should consider the harm lack of independence might cause. If it is significant, other escalation possibilities should be considered. Whistleblowing systems and ethics hotlines, which are generally present in organizations today, can help auditors report any questionable situations they are dealing with without direct confrontation.

Long-term Implications

If an internal auditor is confronted with a situation that impairs his or her independence or that of a team member, and none of the actions taken has resolved the issue, then he or she should consider the long-term implications. As a last resort, an auditor can resign from the job. If an auditor's independence were found to be compromised and he or she was working unethically, the auditor could not only be fired, but he or she could also lose all professional credibility, which can be difficult to regain.

The Basis of Board Trust

The IIA defines *internal auditing* as an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations." Boards of directors rely on internal audit to provide them with reliable information for effective decision-making. This information is most trusted when it comes from an internal audit function that demonstrates its independence. Ia

MAJA MILOSAVLJEVIC, CIA, CRMA, *is an internal auditor at Borealis AG in Vienna, and a 2015* Internal Auditor *Emerging Leader.*

ITAudit

BY KARI ZAHAR + JEREMY PRICE + CURTIS GRIFFIN EDITED BY STEVE MAR

THE HIDDEN RISKS OF THE CLOUD

Internal auditors should review the risks and applications built into Microsoft's widely used computing platform.

Most large organizations are using Microsoft's Azure cloud computing services in one form or another. Indeed, Microsoft claims more than 95% of Fortune 500 companies use Azure. Among other things, Azure supports data analytics, data warehousing, DevOps, storage, virtual desktops, and fully managed infrastructures. Additionally, organizations can integrate the services within Azure into a corporate network in the same way traditional data centers are connected.

Yet, despite Azure's pervasiveness, many organizations don't fully understand the effects the platform may have on daily operations and personnel, or the potential security implications. Azure's services can introduce security and data privacy risks such as inappropriate administrative access, less clarity on role-based access permissions, or inappropriate remote access. For instance, in May 2019, Azure suffered a global outage caused by a domain name system configuration issue, according to Build5Nines.com, which covers cloud technology.

Internal audit can assist the organization in identifying the risks introduced with cloud computing. Partnering with the organization's business units, understanding the technologies, and providing a systematic approach can help to remedy those risks.

First Steps

When auditing Azure, internal auditors should begin by obtaining an inventory of all Azure services in use by the organization. If an inventory does not exist, internal audit can help build one. Auditors can use native reports within Azure or custom scripts to export inventory data from the system.

Next, auditors should understand how these services are implemented, as well as IT's control environment or processes related to cloud services. Are there documented procedures for administering the environment? Is formal change management used in all aspects of the cloud such as networking, storage, maintenance, and provisioning?

For example, with database platform as a service, auditors should understand the database platforms and how they are configured and secured. The organization may set up its own servers in an Azure virtual environment or use Microsoft's Azure SQL server. Each method poses unique audit considerations that need to be investigated.

A third step is performing a risk analysis to determine the risks associated with each of the services and their pervasiveness. Auditors should be aware of how moving these services out of traditional data centers impacts connectivity, communication requirements, separation of duties, latency, response time, administrative security, and

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

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

compliance. Whenever possible, auditors should partner with IT to monitor key performance indicators based on risk to assist with ongoing control monitoring and operations.

A Plan for the Cloud

Once internal auditors have completed these three steps, they are ready to build their audit plan. In doing so, auditors need to address several aspects of the Azure platform.

Azure Security Center Internal audit, IT, or management can quickly identify the organization's Secure Score—which measures its security posture—through the Azure Security Center. The center provides security recommendations based on the organization's current configurations and monitors system updates, vulnerabilities, network security, and other areas.

In addition, Security Center prioritizes recommendations, so auditors know where to start with their assessment. The dashboard groups the organization's security hygiene into categories such as compute and apps, networking, data and storage, identity and access, and security solutions. Auditors should note that the dashboard and associated recommendations are alerts rather than enforced security configurations.

Networking and Virtual Machines Cloud environments can be complex with virtual networking, firewalls, and machines configured from a browser or Microsoft's Azure PowerShell scripting language. Azure administration can be performed via a web browser, and workloads can be administered remotely using many other secure and insecure methods.

Internal audit can help the organization take a strategic approach to risk by validating that remote access to the environment is restricted appropriately and Azure access is secured with multifactor authentication. Simple passwords can be stolen, compromised, or "brute-force" attacked. Once one machine is compromised, it can be used to compromise other Azure resources or attack other networked devices. Multifactor authentication goes beyond passwords by requiring more than one method of authorization for access. In addition to multifactor authorization, all administrative workload access from the internet should be configured for just-in-time security access, which builds secure connections over the internet.

Azure Active Directory With more than one billion user identities hosted, Azure Active Directory is one of the most pervasive organizational risks for businesses using the platform. Services such as SQL databases, data warehouses, and virtual machines all leverage Azure Active Directory, as do Office applications.

Depending on how the organization has implemented Azure Active Directory, it can pose significant administrative access risks. Traditionally, when reviewing administrators for on-premises Active Directory, auditors will evaluate enterprise administrators and domain administrators. However, with Azure Active Directory, there are potentially global administrative accounts. These global accounts could create an account with elevated permissions on the organization's domain. Moreover, they are unlikely to appear in any traditional audit script outputs.

On top of this, in Azure, administrators can create custom groups that have less visibility in the environment. Auditors need to fully understand the risk and compliance implications of these custom groups.

Database Services Depending on how the organization stores its databases within Azure, it may have access to database security features such as logging, log retention, data encryption, and restricted elevated access. Auditors should understand which features are in place and how they are monitored.

Security Assurance

In addition to the security concerns in the previous section, internal auditors should review areas such as data loss prevention, data classification, encryption, and Azure certifications and compliance. Compliance may include the International Organization for Standardization's ISO 27001, System and Organization Control (SOC) reports, the U.S. Health Insurance Portability and Accountability Act, and Payment Card Industry Data Security Standard.

Because these services are complex, internal audit could perform smaller audits around specific areas one at a time. For example, auditors could separate networking, Azure Active Directory, and Security Center into their own audits and prioritize them based on risk. Auditors can leverage free Azure benchmarks issued by the Center for Internet Security and Azure's SOC reports when building out audit plans.

Auditing the Azure environment can be challenging because of the platform's constantly changing and complex design. Internal audit may need to hire outside expertise to evaluate the design and operation of controls in these environments. But by overcoming these challenges and performing audits, internal audit can provide assurance that cloud operations are secure. Ia

KARI ZAHAR *is a senior manager at Stinnett & Associates in San Antonio, Texas, and an accounting analytics professor at Trinity University in San Antonio.*

JEREMY PRICE, CISA, MCSE, ABCP, *is a senior manager at Stinnett & Associates in Tulsa, Okla.*

CURTIS GRIFFIN, GICSP, *is a manager at Stinnett & Associates in Tulsa.*

Risk Watch

BY MELISSA RYAN   EDITED BY RICK WRIGHT

RISK AS THE ROSETTA STONE

Having a common risk language can help an organization facilitate business discussions.

Language determines how people share information, invoke emotion in others, or persuade them to action. The words chosen also frame a listener's perspective on an individual beyond simply that interaction. How people select and use words appropriately in a situation is important.

With this as a backdrop, it was no surprise that when my business partner referred to "risk as the Rosetta Stone" for business, the concept rang true. The Rosetta Stone, discovered in 1799, allowed people to decipher once-challenging Egyptian hieroglyphics. Having the key to deciphering the message unlocked understanding and knowledge previously unavailable.

Using the language of risk offers a similar master decoding structure—in this case, for businesses to leverage for greater understanding. Business demands as varied as resource allocation and product innovation will benefit from the use of a shared risk language that enables the organization to build from a common baseline. Leveraging a common organizational language can increase the organization's efficiency and heighten value delivery. For auditors, leveraging components of a shared language can not only increase message clarity and enable more effective communications with business partners, but also enhance the understanding and outcomes of audits, projects, and advisory engagements.

The Language of Risk

Much as a language is made of key components such as vocabulary (shared definition of words and terms), syntax (arranging words in a sentence for meaning), and pragmatic rules for situational use, the language of risk is made of standard components. Ensuring these components are designed, shared, and understood across the organization supports effective communications and decision-making. Internal auditors should consider how these key risk components are structured in their organization and whether modifications or increased awareness might further enable their use as a common language for the business.

Taxonomies (*a common vocabulary*) The core of any common language leverages a shared baseline. In risk-speak, this baseline is a taxonomy, naming standard, or universe definition. The risk universe or other classification structure provides a consistent lens to assess operational activities, monitor and compare effectiveness, and frame the scope of project or risk remediation efforts. A defined taxonomy also allows for a common aggregated reporting structure. This structure enables effective business decision-making because there is consistency in comparing

SEND RISK WATCH ARTICLE IDEAS to Rick Wright at rick.wright@yrcw.com

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

and contrasting information over time and across organizational functions.

Measurements/Ratings (*a common vocabulary and a guide on syntax and structure*) Prioritization is difficult to define or agree upon without a standard rating scale by which to assess risk. Various functions and teams in an organization often share a scale for rating common risk variables—impact and likelihood. Similarly, internal audit usually defines a rating or prioritization scale for findings and reporting. Other teams, such as enterprise risk or security, also may use rating structures, which may be similar or quite different from others in use. To be able to prioritize and understand risk organization-wide, common scales must be used. When a scale includes metrics that apply cross-functionally—such as financial, operational, regulatory, client, or reputational—it can be better applied and leveraged across functions. For example:

- Apply scale levels to project prioritization based on potential savings or projected revenue increases, or based on customer or marketing impact.
- Apply scale levels to measuring impact and likelihood of audit findings, helping to prioritize resource allocation for remediation efforts.
- Apply scale levels to assessing product opportunities for financial impact, client satisfaction increases, or operational challenge points, aiding in prioritizing focus on go-to-market efforts.

> Enhanced understanding through a common framework can shorten decision-making cycles.

Risk Response/Appetite (*pragmatic rules*) Within an enterprise risk management program, the risk response standard, rules, or matrix guide the norms expected for identified risks. The response standards define when a risk is acceptable within organizational parameters, when action is required, or when a risk is out of bounds but acceptable for monitoring for an interim period. This structure can be applied beyond the risk function to identify points for escalating concerns, engaging management approvals, or prioritizing operational activities.

Business Value of a Shared Language

Leveraging components of the risk language as a Rosetta Stone of understanding can quickly provide value to an organization. Focusing on some key components can enhance communication and improve business functions.

Common Language Enhances Communications Use of a common vocabulary in cross-functional or global communications can ensure the messages reflect a consistent structure and clearly defined operational focus of the organization. The vocabulary should comprise agreed-upon top business risks, common naming, and classification of operational units.

Shared Understanding Improves Efficiencies and Culture Consistent prioritization processes based on a defined measurement scale can increase understanding and alignment among different teams or operational units. While this doesn't necessarily mean a shared agreement is always expected, a shared understanding of the "why" and comfort in consistent prioritization efforts may increase the effectiveness of communications and enhance corporate culture.

Translating Details to Themes Speeds Decision-making Use of a defined risk universe structure in operational functions can provide for aggregation of repeated, consistent individual concern points. Use of the standard universe enables comparison across locations or teams and roll-up of reporting and assessments in a framework that is expected and understood by executive management. Enhanced understanding through a common framework can shorten decision-making cycles and produce solutions faster.

Agreed-upon Prioritization for Resources Enables Quick Time to Value Having standards in place for measurement, response, and escalation can level the playing field, and drive consistent and intentional decision-making for allocating the organization's resources.

Be a Translator

In their role as partners across the organization, internal auditors can promote the common communication and benefits associated with a shared risk language. As audit team members interact with stakeholders and partners, they should share their language with the organization with an eye on promoting understanding, improving efficiencies, and enabling the business. Ia

MELISSA RYAN, CRMA, CISA, *is principal and co-founder at Asureti in Kansas City, Mo.*

BY ANNA KON EDITED BY BRYANT RICHARDS

RUNNING ON EMPTY

A creative salesman manipulates customer profiles to ensure his bonuses during price increases.

At the end of the third business quarter, Sten Lepp, the chief audit executive at NorthStar Energy Corp., received an email from the head of sales, Henry Klassen:

"For your information, on the 8th of July, we discovered that a salesperson, Andy Pine, used standard consumption graphs for certain customers instead of the customers' actual consumption history. Thus, sales to those clients were made with wrong assumptions. As soon as we discovered the manipulation, I had Pine write an explanatory letter and sent him home. We are processing termination documents, and I intend to deduct sales bonuses from his last paycheck to recoup monies. I am truly sorry for the incident. As a manager, it is difficult when a team member breaches trust."

After reading the email, Lepp wanted to better understand exactly how the salesperson manipulated sales. How had such a standardized business process become so trust-based? The email looked like an attempt to sweep the matter under the rug as quickly as possible, so Lepp initiated an internal investigation.

The pricing strategy for each customer was based on the customer's profile. One of the inputs that shaped the profile was the customer's historical energy consumption data, which was used to project future consumption patterns. The pricing model then calculated the minimum selling price, allowing the salesperson to add a margin to that price while maintaining customer relations. This margin was shared between the salesperson and the company, and the salesperson's bonus was a percentage of the added margin.

In the previous year, energy market prices increased, resulting in a higher precalculated base selling price. Most of the sales team was struggling to add every cent to the sales margin without customers complaining about the cost increases. Pine, however, completed contracts and bragged about his bonuses. His colleagues grew curious, but no one dared to ask Klassen because of his close friendship with Pine. Their chance came when Klassen left for a scheduled vacation and Helina Saar, a recent hire, came in as his temporary replacement.

When the other salespeople approached Saar about the discrepancies in bonuses, she accessed Pine's portfolio in the sales system and found that he used creative solutions to ensure his bonuses while his co-workers struggled. Specifically, he changed the presumably unchangeable—the customer's profile. He manually changed inputs to the pricing model in the sales system. Instead of using the customer's real

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

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

LESSONS LEARNED

- » Don't jump to conclusions. Just because the prime suspect was no longer with the company and Klassen assured everyone that the incident had been taken care of doesn't mean there isn't much to investigate. When beginning an investigation, avoid assessments and conclusions early on and keep an open mind.
- » Use professional skepticism, instead of falling victim to truth bias, which is people wanting to believe what they see or hear. The investigators first interviewed Klassen, who was cooperative and ready to explain the sales process and fraud scheme. While the chief investigator then compiled a summary of Pine's deeds, the effective resolution, and the incident's low impact, the other investigation team member decided to talk to the portfolio analyst. By talking to the analyst, the investigator learned that Klassen was not telling the truth and that the loss from those contracts was more substantial than a single person's bonuses. The analyst also revealed that Pine and Klassen were close friends.
- » Have a thorough investigation plan. List all employees to be interviewed and in what order. Never start with those who could potentially be main suspects. Had the auditor not decided on her own to talk to the portfolio analyst, he never would have discovered that Klassen was less than truthful. Make sure investigation steps and responsibilities are listed, as well as what evidence is most likely needed. Agree ahead of time on communication channels and frequency, where evidence is stored and how it is indexed, and set and monitor deadlines for each step of the investigation.
- » Understand business context. Klassen succeeded in undermining the impact of the fraud because he focused everybody's attention on bonuses overpaid to a single salesperson rather than the lack of controls withinin the sales system. If you are not familiar with the business, step back to read through manuals and related procedures, and interview employees.
- » Conduct due diligence by preserving evidence. The decision to turn the case over to law enforcement may be reached several months later, but the evidence should still be available and the chain of custody must be clear.

historic consumption data, Pine entered the customer's consumption as a single value, so the system disregarded real consumption patterns and distributed consumption equally, calculating lower base prices. Lower base prices allowed Pine to add the desired margin and receive a larger bonus from each sale.

Saar talked about her findings with the portfolio analyst responsible for monthly sales results reporting, who then approached her supervisor to confirm the findings. The supervisor waited until Klassen returned from his vacation and informed him about Pine's contracts. Klassen had no choice but to fire Pine.

The investigation unveiled several key findings:

- » The sales process manual had not been reviewed for more than five years, and actual practices deviated substantially. There were no controls or monitoring from the head of sales or anyone else.
- » No attention was paid to the development of the sales information system. As a result, IT controls were not performing as intended and could be easily overridden with no one noticing.
- » Bonuses were paid out immediately based on forecasted revenues, and actual execution of sales contracts were not monitored, which invited fraudulent behavior from sales personnel.
- » Klassen and Pine owned and ran an online retail business together. Though it was in an unrelated business sector and did not breach NorthStar's code of conduct, the investigation found that they took care of their affairs during business hours. Therefore, Klassen was paying little attention to what was going on in the sales unit.
- » NorthStar, of course, suffered losses from such deals as it will have to cover energy costs from the customers' real consumption patterns.

As a result, the company completely restructured the sales process, supporting information system, and bonus principles; contacted law enforcement; reviewed whistleblowing channel effectiveness; and fired Klassen. Ia

ANNA KON, CIA, CRMA, CFE, *is a head of internal audit in Tallinn, Estonia.*

Risks

Over the past several decades, the spotlight on corporate governance has intensified as organizations realize the criticality of managing risk and making well-informed, strategic decisions. But despite widespread adoption and implementation of corporate governance models, the health of corporate governance isn't where it should be, according to a recent study from The IIA. OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk investigates how far the three main pillars of corporate governance—executive management, the board, and internal audit—are aligned when it comes to understanding and managing risk. The report uncovers a pervasive lack of communication and coordination among those groups in key risk areas organizations are likely to face in 2020 and beyond (see "Key Findings" on page 24).

Boards were found to be more confident than executive management that their businesses are capable of addressing threats in nearly every one of the 11 risks examined. Moreover, internal audit and the board share similar views on their organizations' level of risk management maturity, generally

BASE PORTRAITS FROM LEFT TO RIGHT: ROMAN SAMBORSKI, STUART JENNER, LEUNGCHOPAN, ANTHONY BOLAN, LJUPCO SMOKOVSKI, PANICATTACK / SHUTTERSTOCK.COM

in View

Arthur Piper

Illustration by Sean Yates

A recent survey highlights the often wide disconnect among organizational stakeholders on key risk areas.

rating those capabilities higher than executive management in most areas. And while the findings highlight a troubling disconnect among the three groups surveyed, they also point to opportunities for internal auditors to help bridge knowledge gaps among the organization's key decision-makers.

LACK OF ALIGNMENT

Worryingly, most businesses lack alignment around the knowledge and capabilities needed to address risk. Jim Pelletier, The IIA's vice president, Professional Standards and

Knowledge, says that finding should be ringing alarm bells across corporate America. Given that the C-suite is responsible for the day-to-day management of risk and for setting a strategy to cope with those threats, their consistently more pessimistic view of their organization's capacity to do so effectively is likely to be in touch with the realities on the ground.

"What the report really points out is that internal audit is not playing the critical role it ought to play," Pelletier says. "Boards should, of course, rely heavily on management, but relying on management alone is incomplete. Boards need to turn to a source independent from management — internal audit — for assurance that the information they are receiving is complete, accurate, and reliable." While failure to do so could indicate lack of maturity of the internal audit function's role — the survey found one-third of organizations have no systematic approach to risk management — it also suggests the benefits an independent audit function can bring are not understood by the board.

While IIA surveys confirm that most internal audit functions report administratively to the audit committee, the reality, according to Pelletier, is that many audit committees are shirking their oversight responsibilities and pushing internal audit down in the organization. Boards that allow this to happen, he adds, are missing the critical perspective that a correctly placed, well-resourced audit function can provide.

"When the board is clear that it wants a strong, independent internal audit function that can look across the organization and ensure it is getting all of the information it needs for good decision-making, it won't get that from an audit function that is simply there to take care of complying with the requirements of the U.S. Sarbanes-Oxley Act of 2002," Pelletier says. "Boards are missing out on the opportunity to leverage internal audit as a tool to help them become stronger."

KEY FINDINGS

The OnRisk 2020 report identifies seven key findings that provide insight on respondents' understanding of risk and their perceptions of how those risks are managed:

- Boards are overconfident because they consistently view the organization's capability to manage risks higher than executive management.
- Boards generally perceive higher levels of maturity in risk management practices than executive management and chief audit executives.
- "Acceptable misalignment" on risk is a prevalent and dangerous mindset, with some respondents describing such misalignment as "healthy."
- Some industries are lagging in adopting systematic approaches to risk – particularly in the health-care, retail/wholesale, and public sectors.
- Cybersecurity, data, and new technologies represent critical knowledge deficits.
- Data and new technologies, data ethics, and sustainability risks are expected to grow in relevance.
- Talent management and retention is at the center of future concerns, with the inability to attract and retain business-critical skills emerging as a key risk.

RISK GOVERNANCE

Many survey respondents played down the significance of a misalignment in understanding risk among the three groups — often saying it was a healthy state of affairs. The respondents' ratings of their personal knowledge of each risk were, in fact, closely aligned. But in many areas, their reported understanding of how well the organization could manage risk varied widely.

"I believe it is healthy to look at something through different lenses and assess risk through those different lenses," says Mark Carawan, chief compliance officer and former chief auditor at Citigroup in New York. Geography, product sets, and legal entities, for instance, can all provide useful constructs through which to consider risk. "But if it is real misalignment, that points to a lack of a proper risk governance framework, common risk taxonomies, a well-articulated risk appetite, and agreed and consistently applied key risk indicators — so you can identify, measure, monitor, report, and control risks in a way that everyone understands," he says.

Carawan adds that without an effective risk management framework, clear communication among the three groups surveyed is impossible. CAEs can readily assess the state of their organizations' risk governance framework and its relation to the articulation and measurement of risk through an audit. But the task of understanding how well the whole gamut of risks the business faces is linked to a well-articulated risk appetite is problematic — the world's business landscape is dynamic and complex, producing new risks regularly. Audit reports must articulate whether the business is on track to meet its strategic goals within the risk appetite.

"That is one of the tough things for an auditor to achieve, because what

Less than one-quarter of organizations worldwide quantify their top 10 risks, according to Aon's 2019 Global Risk Management Survey.

one does is very focused on the tactical execution of different audit procedures and on producing an audit report," Carawan says. "The output of the audit doesn't have anywhere near the impact that it should if it is not linked to the outcome for the organization, the client, and the success of the firm and how it manages risk—particularly in stress scenarios." Even in audit planning, internal auditors need to make sure they are looking at key risks rather than at the key processes—strategic issues, not tactical ones.

For instance, OnRisk 2020 identifies regulatory change as one of the areas of greatest misalignment in terms of perceived organizational risk management capacity. Only one-third of C-suite respondents feel confident they are doing well in this area, whereas two-thirds of CAEs rate their capability as good.

"The volume of regulatory change can present challenges for many organizations," Carawan says. "But it's critical to make sure that it is well-monitored, measured, and reported. In many cases, this is a significant risk area that has been underexplored by the third line of defense." Boards should have available for review an inventory of regulations mapped onto the organization's processes and controls, as well as clear metrics for the rate of regulatory change, he says. While government officials announce planned new legislation well in advance, such as Europe's General Data Protection Regulation (GDPR), the detailed requirements may only appear near, or even after, the legislation actually goes into effect. That means key risk areas likely have not been identified and are not subject to adequate, timely risk management oversight and control—unless the CAE strives to stay on top of regulatory developments.

PERSISTENTLY BEHIND

CAEs surveyed by The IIA predict that, by 2024, the top three most relevant risk areas will be technological (see "Present and Future Risks" on page 27). It cites data and new technology, and data ethics, as the fastest rising risks—leaping 18 and 15 percentage points, respectively, in the next five years. "Technology and digital innovation are evolving at a rapid pace—much faster than ever before," says Christa Steele, a California-based board director on both New York Stock Exchange listed companies and privately owned businesses. "This is a game changer for tried and true business models—it is no longer business as usual. A lot of boardrooms are not current on the pace of industry change, and the same can be said about some C-suites. Yet, all industries are being disrupted."

Changes are so rapid that boards don't know what questions to ask.

In many sectors, competition and technology are changing so quickly that boards simply do not understand what questions to ask, Steele says. The report says this knowledge gap stems in part from a lack of board education, as well as insufficient communication among the three groups surveyed.

"One thing that would be highly valuable for the board to ask the CAE in executive session is to give an overview of his or her thoughts on what the risks look like in the company," she

"Boards are missing out on the opportunity to leverage internal audit as a tool to help them become stronger."

Jim Pelletier

"The output of the audit doesn't have anywhere near the impact that it should if it is not linked to the outcome for the organization."

Mark Carawan

MORE VISIT http://bit.ly/OnRisk2020 to download a copy of OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk.

"The CAE needs to have a shift in mindset, which is to move away from just reporting past findings and, instead, interpret, predict, and prevent risk."

Christa Steele

"The problem is we are often employing old tools to deal with these new constructs, which makes it very difficult to manage today's risks effectively."

Dominique Vincenti

says. "The CAE has the best visibility with the largest number of boots on the ground to surveil risk. I think the CAE is underutilized right now." Now that she is working as a board member, Steele adds, she has a greater appreciation for what a pivotal role the CAE can play—not just in overseeing and communicating on risk, but in setting up educational sessions with the board to talk about the wider risk landscape and to use recent news headlines involving poor company decision-making that might provide useful lessons. But her enthusiasm is tempered by a caveat.

"The CAE needs to have a shift in mindset, which is to move away from just reporting past findings and, instead, interpret, predict, and prevent risk," she says. "If we can get that mindset at the CAE level, at the C-suite level, and at the board level, then we create better alignment."

For its part, the board also has to step up and make sure the CAE and internal audit have the right kind of key performance indicators and key risk indicators.

"I've spent a significant amount of time in Silicon Valley working with early- to late-stage startups across a variety of industries," she says. "This time in my life has forever changed how I think with regard to business operations and digital disruption—I encourage the C-suite, the CAE, and the board to do the same. Communication and transparency are key. Better communication comes from better education and dialogue."

TECHNOLOGY RISK

Cybersecurity ranks as the most relevant risk to tackle by all groups both now and in the future, according to the report. Yet while cyber breaches are a prevalent reality in business life, the threat is as old as the internet itself—so why do businesses say they find it so hard to deal with? The OnRisk survey suggests that, due to a lack of knowledge within the internal audit team, some CAEs rely too much people and budget dollars allocated to innovation and the transitional risk oversight caused by new innovation in the business. She agrees with Pelletier that too many boards—and specifically audit committees—are heavily driven by Sarbanes-Oxley in the way they use the internal audit function. To broaden board thinking, Steele says board members need to get educated on the uses of artificial intelligence, data aggregation, predictive analytics, and blockchain and to understand how these technologies impact their company business models. Only then can board oversight encompass the on assurance from the chief information security officer that controls around cyber risk are sound. It is an explanation that Dominique Vincenti, global head of internal audit–chief audit executive at Uber in San Francisco does not accept.

"Knowing what to do in this field has been understood for years," she says. "CAEs are well-equipped with lots of robust frameworks—such as the [U.S. National Institute of Standards and Technology (NIST)] Cybersecurity Framework and the Sender Policy Framework for email—to help them ask the right questions. It is

Cybersecurity ranks as the most relevant risk to tackle by all groups.

Issues associated with **digitalization** comprise the top **concerns** identified by senior executives worldwide in Gartner's third-quarter 2019 Emerging Risks Monitor Report.

PRESENT AND FUTURE RISKS

In-depth interviews with board members, senior management, and chief audit executives for the OnRisk 2020 report yielded a ranking of top risks facing organizations today and tomorrow.

RISK RANKINGS BY RELEVANCE

2020	2024
1. Cybersecurity (86%)	1. Cybersecurity (90%)
2. Data protection (78%)	2. Data protection (85%)
3. Regulatory change (66%)	3. Data and new technology (82%)
4. Business continuity (65%)	4. Business continuity (67%)
5. Data and new technology (64%)	5. Third party (66%)
6. Third party (60%)	6. Regulatory change (64%)
7. Talent management (58%)	7. Talent management (65%)
8. Culture (57%)	8. Data ethics (66%)
9. Board information (54%)	9. Culture (58%)
10. Data ethics (51%)	10. Board information (51%)
11. Sustainability (30%)	11. Sustainability (45%)

the topic most written about with the most guidance available, so there is really no excuse. That's why I call it negligence."

Cyber-risk expertise should be no less difficult to understand than legal risk, for Vincenti, because she does not see it as the CAE's job to be a subject-matter expert in anything other than risk management. As risks evolve and become more complex, it is up to the CAE to continually restructure his or her team with the right skills and expertise needed. For the CAE, she says, the question should be, "Am I building the team I need to do the job in today's context?" Addressing the talent management issue identified by the survey requires internal audit leaders to think more laterally about the staff they hire.

Like Steele, Vincenti says the crux of the problem is that many boards, C-suite executives, and CAEs have not caught up with the fundamental structural change digitalization implies—especially in areas such as third-party risk where problems need to be reframed. "For me, when people talk about third-party risks, it shows me that they are already 10 years in the past," she says. "We are not dealing with third parties anymore—we are working in ecosystems and on platforms where we are interconnected and interdependent. The problem is we are often employing old tools to deal with these new constructs, which makes it very difficult to manage today's risks effectively."

She accepts it is not always easy to get such messages across and has had personal experience failing to convince boards and C-suites to act on emerging issues in previous roles. In one organization, she repeatedly told management that it needed to care more about data privacy and was repeatedly ignored. Later, when preparing for GDPR, the company found its data privacy processes to be relatively poor. She jokes that she felt like the ancient Greek seer Cassandra who warned the Trojans not to accept the gift of a giant wooden horse—it was secretly packed with heavily armed Greek warriors—because it would lead to the sacking of the city of Troy. But she sees providing foresight as a critical role for internal audit to play and devotes one-third of every executive meeting to emerging issues—often repeating the same material if she thinks inadequate action has been taken.

TIME TO ACT

The world may have changed radically over the last few decades, but the need for effective risk management has not. If the corporate governance model is to work well, CAEs need to play their part more effectively. They not only need to understand today's business environment, build the right audit teams, and use cutting-edge tools to deal with complex and interconnected risks, but they also must be outspoken and resilient enough to press their organizations to act on the emerging threats on the horizon.

While there is work to do, the paths that each of the three groups surveyed in the report must follow are relatively clear, according to those interviewed. Communication on risk must be clear and unambiguous, underpinned by an effective risk governance framework. The C-suite needs to bring the CAE's team in early on key strategic issues. The board needs to make sure the internal audit function is well-resourced to deal with strategic risks and innovation, rather than relegating the department to play only a compliance role. Perhaps many people in corporate America already thought the way business leaders communicate and act on risk within their organizations was out of kilter. The OnRisk 2020 survey provides the objective evidence that such misalignment on risk is real. It is time to act on that knowledge.

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

LYNDON Group

Does your organization use SAP Concur?

Spend Management Auditing

Outsource or Co-Source your Audit to Lyndon Group:

OPERATIONS

- Efficiency
- Savings
- Usability

REPORTING

- Allocations
- Analytics
- Reconciliations

COMPLIANCE

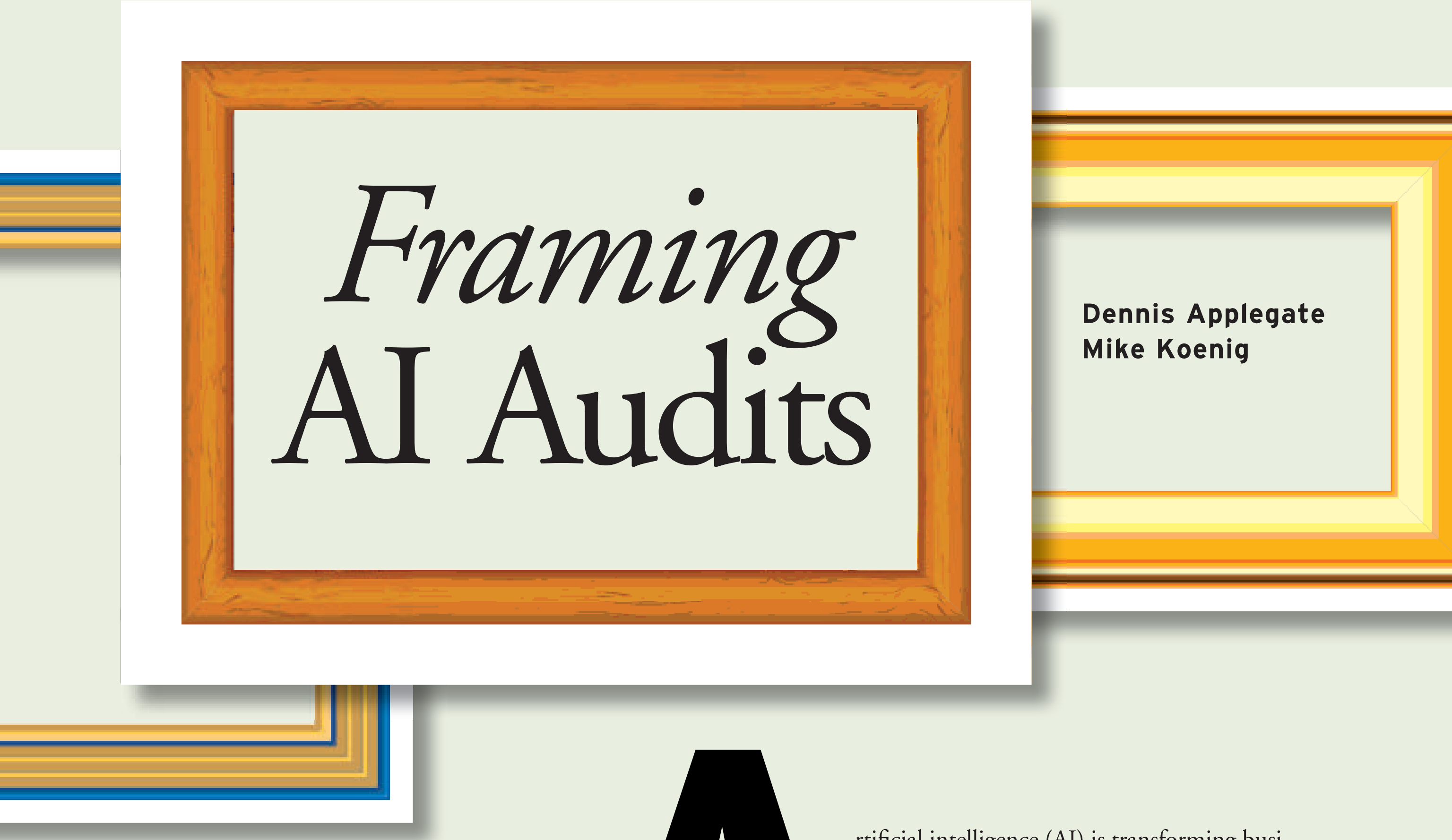
- Contracts
- Policies
- Regulatory

Learn more at
www.lyndon-group.com/auditservices

SAP® Concur® Partner
Solution Provider

SAP® Concur® Partner
Customer Success

Follow us @Lyndon-Group



Framing AI Audits

Dennis Applegate
Mike Koenig

As more organizations implement artificial intelligence, internal auditors need a framework for reviewing these systems.

Artificial intelligence (AI) is transforming business operations in myriad ways, from helping companies set product prices to extending credit based on customer behavior. Although still in its nascent stage, organizations are using AI to rank money-laundering schemes by degree of risk based on the nature of the transaction, according to a July EY analytics article. Others are leveraging AI to predict employee expense abuse based on the expense type and vendors involved. Small wonder that McKinsey & Company estimates that the technology could add $13 trillion per year in economic output worldwide by 2030.

If AI is not on internal audit's risk assessment radar now, it will be soon. As AI transitions from experimental to operational, organizations will increasingly use it to predict outcomes supporting management decision-making. Internal audit departments will need to provide management assurance that the predicted outcomes are reasonable by assessing AI risks and testing system controls.

EVOLVING TECHNOLOGY

AI uses two types of technologies for predictive analytics—static systems and machine learning. Static systems

ANNA CHELNOKOVA / SHUTTERSTOCK.COM

are relatively straightforward to audit, because with each system iteration, the predicted outcome will be consistent based on the datasets processed and the algorithm involved. If an algorithm is designed to add a column of numbers, it remains the same regardless of the number of rows in the column. Internal auditors normally test static systems by comparing the expected result to the actual result.

By contrast, there is no such thing as an expected result in machine learning systems. Results are based on probability rather than absolute correctness. For example, the results of a Google search that float to the top of the list are those that are most often selected in prior searches, reflecting the most-clicked links but not necessarily the preferred choice. Because the prediction is based on millions of previous searches, the probability is high—though not necessarily certain—that one of those top links is an acceptable choice.

Unlike static systems, the Google algorithm, itself, may evolve, resulting in potentially different outcomes for the same question when asked at different intervals. In machine learning, the system "learns" what the best prediction should be, and that prediction will be used in the next system iteration to establish a new set of outcome probabilities. The very unpredictability of the system output increases audit risk absent effective controls over the validity of the prediction. For that reason, internal auditors should consider a range of issues, risks, controls, and tests when providing assurance for an AI business system that uses machine learning for its predictions.

AI SYSTEM DEVELOPMENT

The proficiency and due professional care standards of the International Professional Practices Framework require internal auditors to understand AI concepts and terms, as well as the phases of development, when planning an AI audit (see "Three Phases of Development" on this page). Because data fuels these systems, auditors must understand AI approaches to data analysis, including their effect on the system algorithm and its precision in generating outcome probabilities.

Features define the kinds of data for a system that would generate the best outcome. If the system objective is to flag employee expense reports for review, the features selected would be those that help predict the highest payment risk. These could include the nature of the business expense, vendors and dollar amounts involved, day and time reported, employee position, prior transactions, management authorization, and budget impact. A data scientist with expertise in this business problem would set the confidence level and predictive values and then let the system learn which features best determine the expense reports to flag.

Labels represent data points that a system would use to name a past outcome. For instance, based on historical data, one of the labels for entertainment expenses might be "New York dinner theater on Saturday night." The system then would know such expenses were incurred for this purpose on that night in the past and would use this data point to predict likely expense reports that might require close review before payment.

Feature engineering delimits the features selected to a critical few. Rather than provide a correct solution to a given problem, such as which business expense reports contain errors or fraud, machine learning calculates the probability that a given outcome is correct. In this case, the system would calculate which expense reports are

THREE PHASES OF DEVELOPMENT

The chart below condenses the development phases of AI systems.

TRAINING PHASE

» Extract datasets from multiple, diverse systems as required.

» Define features and labels through expert analysis.

» Train system to connect features and labels using the extracted datasets.

TESTING PHASE

» Refine system algorithm using control datasets.

» Perform feature engineering on the system to narrow down the number of features.

» Identify the critical features using data analysis and expert judgment.

PRODUCTION PHASE

» Make the system's predictive models available to users for decision-making.

» Ensure user access controls are in place.

» Track the quality of the user experience via performance metrics.

37% of U.S. executives say ensuring AI systems are trustworthy is a top priority, and 64% are boosting AI security with validation and monitoring, says PwC's 2019 AI Predictions.

likely to contain the highest probability of errors or fraud based on the features selected. The system then would rank the outcomes in descending order of probability.

Machine learning involves merging selected features and outcome labels from diverse datasets to train a system to generate a model that will predict a relationship between a set of features and a given label. The resulting algorithm and model are then refined in the testing phase using additional datasets. This phase may consider hundreds of features at once to discover which features yield the highest outcome probability based on the assigned labels.

Feature engineering then deletes the number of system features to enhance the precision of the outcome probabilities. Based on the testing phase, for example, the nature of the expense, the dollar amounts involved, and the level of the employee's position may best indicate high-risk business expense reports requiring close review. During the production phase, as the system calculates the risk of errors and fraud in actual expense reports, it may modify the algorithm based on actual output probabilities to improve the accuracy of future predictions. Doing so would create continuous system learning not seen in static systems.

In AI system development, it is important for organizations to establish an effective control environment, including accountability for compliance with corporate policies. This environment also should comprise safeguards over user access to proprietary or sensitive data, and performance metrics to measure the quality of the system output and user acceptance of system results.

A RISK/CONTROL AUDIT FRAMEWORK

Nine procedures frame the audit of an AI system during the training, testing, and production phases of development. The framework provides a point of departure for AI audit planning and execution. Assessed risk drives the controls expected and subsequent internal auditor testing.

Internal auditors may need to adjust the procedures based on their preliminary survey of the AI system under audit, including a documented understanding of the system development process and an analysis of the relevant system risks and controls. Moreover, as auditors complete and document more of these audits, it may be necessary to adjust the framework.

Normally, internal auditors adjust their assessment of risk and their resulting audit project plans based on observations made in the preliminary audit survey. The boxes, starting on page 32, depict conditions that may alter assessed risk as well as modify expected AI system controls and subsequent audit testing during specific phases of development.

Data Bias (Training Phase) Use of datasets that are not representative of the true population may create bias in the system predictions. Bias risk also can result from failing to provide appropriate examples for the system application.

A control for data bias is to establish a system review and approval process to ensure there are verifiable datasets and system probabilities that represent the actual data conditions expected over the life of the system. Audit tests of control include ensuring that:

- Qualified data scientists have judged the datasets.
- The confidence level and predictive values are reasonable given the data domain.
- Overfitting has not biased system predictions.

Data Recycling (Training) This risk can happen when developers recycle

MORE

VISIT http://bit.ly/AITerms to read "Getting to Know Common AI Terms."

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

the wrong datasets for a new application, or impair the performance or maintenance of existing systems by using those datasets to create or update a new application.

One control for data bias is independently examining repurposed data for compliance with contractual or other requirements. In addition, organizations can determine whether adjustments in the repurposed data have been made without impacting other applications.

Examples of control tests are:

- Evaluating the nature, timing, and extent of the independent examinations.
- Testing the records of other applications for performance or maintenance issues that stem from the mutually shared datasets.

Data Origin (Training) Unauthorized or inappropriately sourced datasets can increase the risk of irrelevant, inaccurate, or incomplete system predictions during the production phase.

To control this risk, the organization should inspect datasets for origin and relevance, as well as compliance with contractual agreements, company protocols, or usage restrictions. The results of these inspections should be documented.

To test controls, auditors should:

- Review data source agreements to ensure use of datasets is consistent with contract terms and company policy.
- Examine the quality of the inspection reports, focusing on the propriety of data trimmed from the datasets.

Data Conclusion (Testing Phase) Inappropriately tested data relationships could result in improper system conclusions that are based on incorrect assumptions about the data. These conclusions could create bias in management decisions.

The control for this risk is to ensure each feature of the system contains data for which the purpose has been approved for use. Developers should assess the results of such data for misinterpretation and correct it, as appropriate.

Testing this control involves reviewing user interpretations and subsequent management decisions based on system predictions. By performing this test, organizations can ensure that the data supports the conclusions reached and decisions made by management.

Data Overfit (Testing) With this issue, the risk is that datasets may not reflect the actual data domain. Specifically, data outliers may have been trimmed during system testing, leading to a condition that overfits the algorithm to a biased dataset. That could cause the system to respond poorly during the production phase.

Organizations can control for this risk by validating datasets in system testing to ensure that the samples used represent all possible scenarios and that the datasets were modified appropriately to obtain the currently desired system outcome.

To test this control, internal auditors should review all outlier, rejected, or trimmed data to ensure that:

- Relevant data has not been trimmed from datasets.
- Datasets remain locked throughout testing.
- The algorithm has processed the data in an unbiased way.

Data Validation (Testing) Failure to validate datasets for integrity through

TRAINING PHASE

Considerations for adjusting the assessed level of AI audit risk include:

- If system reviews are in place to evaluate training data modifications, deletions, or trimming, this condition should help prevent overfitting the training dataset to generate a desired result, reducing audit risk.
- New AI systems may use datasets of existing systems for reasons of time and cost. Such datasets, however, may contain bias and not include the kinds of data needed to generate the best system outcomes, increasing audit risk.
- AI datasets that consist of numerous data records should contain some errors. In fact, an error-free dataset would indicate a bad dataset, because the occurrence of errors should match the natural rate. For example, if 5% of employee expense reports are filled in incorrectly and are missing key data, then the training dataset should contain a similar frequency. If not, then audit risk increases.

54% of employers say they aren't concerned that the organization could use AI unethically, and only 23% have a written policy for using AI ethically, according to software firm Genesys.

TESTING PHASE

Considerations for adjusting the assessed level of AI audit risk include:

- If independent, third-party judges tested the system data, but no process is in place to reconcile differences in test results between judges, then audit risk increases.
- Because system predictions are based on probability, perfect test results are not possible. If third-party judges evaluating the test results find no issues, then data overfit may have occurred, increasing audit risk.
- If the system has not been validated to prevent user misinterpretations caused by incorrect data relationships, such as flagging business expense reports based on employee gender, then audit risk increases. Alternatively, if user interpretations based on system predictions have not been validated to ensure system data supports the interpretation, then audit risk also increases.
- If data scientists fail to use representative datasets with examples involving critical scenarios to train the system, then audit risk increases.
- If the datasets are not locked during testing, then the data scientist may adjust the algorithm to inadvertently process the data in a biased manner, increasing audit risk.
- If the datasets are locked during testing, but the data scientist fails to review the actual system prediction for integrity, then audit risk increases.

automated systems or independent, third-party judges can lead to unsupported management decisions or regulatory violations. An example would be allowing the personal data of European Union (EU) citizens to be accessed outside of the EU in violation of Europe's General Data Protection Regulation.

Organizations can control for this risk by implementing a validation process that compares datasets to the underlying source data. If the organization uses automated systems, it should ensure the process reveals all underlying issues affecting the quality of the system output. If the organization uses independent, third-party judges, it should ensure the process allows judges the access they need to the raw data inputs and outputs.

To test these controls, internal auditors should:

- Assess the process and conditions under which the validation took place, assuring that all high-risk datasets used in the system were validated.
- Confirm randomly selected datasets with underlying source data.
- When datasets are based on current system data, validate such data is correct to avert a flawed assessment of actual system data.

Data Processing (Production Phase) Failing to validate internal systems processing can cause inconsistent, incomplete, or incorrect reporting output and user decisions. However, periodically reviewing and validating input and output data at critical points in the data pipeline can mitigate this risk and ensure processing is in accordance with the system design.

Auditors can test this control by:

- Reconstructing selected data output from the same data input to validate system outcomes.
- Performing the system operation again.
- Using the results to reassess system risk.

Data Performance (Production) If there is a lack of performance metrics to assess the quality of system output, the organization will fail to detect issues that diminish user acceptance of system results. For example, an AI system could fail to address government tax or environmental regulations over business activity.

Controlling data performance risk requires organizations to establish metrics to evaluate system performance in both the training and production phases. Such metrics should include the nature and extent of false positives, false negatives, and missed items. In addition, developers should implement a feedback loop for users to report system errors directly, among other performance measures.

To test these controls, internal auditors should:

- Examine reported variances from established performance measures.
- Test a representative sample of performance variances to confirm whether management's

PRODUCTION PHASE

Considerations for adjusting the assessed level of AI audit risk include:

- Systems that leverage the datasets of existing systems already audited should lower overall audit risk and not require as much audit testing as new systems using datasets not previously audited.
- Systems that process inputs and outputs at all stages of the data pipeline should facilitate validation of system-supported user decisions and lower overall audit risk. However, if data inputs and outputs are processed in a black-box environment, confirming internal system operations may not be possible. That would increase the audit risk of drawing the wrong conclusion about the reasonableness of the system output.
- If performance metrics are used to measure the quality of the data output, user acceptance of system results, and system compliance with government regulations, then audit risk decreases.
- If performance metrics monitor both system training and production data, then audit risk decreases.
- If performance metrics measure system accuracy but not precision, overlooking a possible system performance issue, then audit risk increases.
- Well-designed systems prevent unauthorized access to system data based on company protocols and regulatory requirements and routinely monitor access for security breaches, decreasing audit risk.

follow-up or corrective action was appropriate.

- Determine whether such action has enhanced user acceptance of system results.

Data Sensitivity (Production) With this issue, the risk is unauthorized access to personally identifiable information or other sensitive data that violates regulatory requirements. Controls include ensuring documented procedures are in place that restrict system access to authorized users. Additionally, ongoing monitoring for compliance is needed. Control testing includes:

- Comparing system access logs to a documented list of authorized users.
- Notifying management about audit exceptions.

ALGORITHMIC ACCOUNTABILITY

As AI technology matures, algorithmic bias in AI systems and lack of consumer privacy have raised ethical concerns for business leaders, politicians, and regulators. Nearly one-third of CEO respondents ranked AI ethics risk as one of their top three AI concerns, according to Deloitte's 2018 State of AI and Intelligent Automation in Business Survey.

What's more, the U.S. Federal Trade Commission (FTC) addressed hidden bias in training datasets and algorithms and its effect on consumers in a 2016 report, Big Data: A Tool for Inclusion or Exclusion? Such bias could have unintended consequences on consumer access to credit, insurance, and employment, the report notes. A recent U.S. Senate bill, the Algorithmic Accountability Act of 2019, would direct the FTC to require large companies to audit their AI algorithms for bias and their datasets for privacy issues, as well as correct them. If enacted, this legislation would impact the way in which such systems are developed and validated.

Given these developments, the master audit plan of many organizations could go beyond rendering assurance on AI system integrity to evaluating compliance with new regulations. Internal auditors also may need to provide the ethical conscience to the business leaders responsible for detecting and eliminating AI system bias, much as they do for the governance of financial reporting controls.

These responsibilities may make it harder for internal audit to navigate the path to effective AI system auditing. Yet, those departments that embark on the journey may be rewarded by improved AI system integrity and enhanced professional responsibility.

DENNIS APPLEGATE, CIA, CPA, CMA, CFE, *is a lecturer in internal auditing and accounting at Seattle University and served on the management team of Boeing Corporate Audit for 20 years.*

MIKE KOENIG *is a lecturer in computer science at Seattle University and was a software engineering and AI leader at Microsoft for 25 years, with 19 patents.*

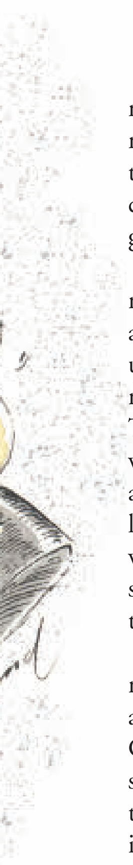
DON'T JUST FOLLOW RULES.
HAVE STANDARDS.

Internal auditors should BE BRAVE

Telling the truth and presenting the facts sometimes requires an act of courage.

Norman Marks

Illustrations by Gary Hovland



“You can’t say that!”

My boss, the chief audit executive (CAE), was telling me to change the audit report. For the second year in a row, my team found that accounting was not performing important reconciliations on time. As a result, financial reporting could be materially misstated and significant fraud might go undetected.

Rather than simply advising on-time completion of reconciliations, the audit team had performed a root cause analysis. They found that, due to cost-cutting, staffing in the unit responsible for the reconciliations had not only been reduced but also tasked with numerous special projects. The unit lacked sufficient people to meet its responsibilities without significant overtime, which management would not approve. Even if it did, the level of overtime would inevitably lead to burnout and the loss of valuable employees. Although we had found deficiencies relating to reconciliations, the staffing issue might affect the performance of other important controls.

The draft audit report explained that insufficient resources had elevated the unit’s risk level and recommended adding permanent staff or contractors at month-end. The CAE, however, was reluctant to include that information. He said that his name was on the audit report, and he refused to recommend an action he was sure management would ignore. In fact, management would be angry that we had questioned its cost-cutting strategy. We delivered the report without identifying the root cause and merely recommended completion of the reconciliations.

The original report was correct, explained the business risk, and recommended appropriate corrective actions. But perhaps because he feared how management would react, the CAE kept part of the story—part of the risk—to himself. The CAE, in other words, was not brave.

It can be hard for internal auditors to tell their stakeholders, whether at the board level or in top management, what is putting the organization at greatest risk. It can be hard to say that control failures stem from insufficient staffing, inadequate pay, or imperfect leadership. It can be hard to say that the organization’s structure, processes, people, and methods are not agile enough to succeed in today’s dynamic world. But these are all truths that need to be told. If no one tells the emperor he has no clothes, he will carry on without them.

Internal auditors at every level are subject to all kinds of pressure that may inhibit them from speaking out. Yet if they are to be effective, they must be able to do so—even at great personal risk.

THE INEFFECTIVE MANAGER

A few years later, when I served as CAE at another organization, I tasked my team with an audit of the Commercial Accounting function. Significant billing errors had been made, and our priority was to find out why.

When we interviewed the department head, a rising star at the company, he explained that errors had been made because his employees were incompetent. Not a single accountant had passed the CPA exam. As a result, he had

to do all the challenging tasks himself, requiring him to work many hours each day and most weekends. Mistakes were inevitable. He asked that we recommend human resources change the job requirements to include a CPA or equivalent.

> “You gain strength, courage, and confidence by every experience in which you really stop to look fear in the face. ... You must do the thing you think you cannot do.” –Eleanor Roosevelt

The audit lead asked me if we could make such a recommendation. His team confirmed that the department head was Commercial Accounting’s only CPA and that the function often needed to perform complex accounting tasks. I told him to speak with each of the Commercial Accounting staff members and form his own opinion on whether they were competent to perform the work.

The interviews went well. I was surprised to learn that the staff had many years’ experience in commercial accounting, including the more complex tasks the department head said they were not competent to perform. The employees were proficient, but their manager did not allow them to make decisions. In fact, he gave them simple assignments and never explained what he was trying to accomplish. Many of the employees were frustrated and considering leaving the company.

The department head was the root cause of the control failures. The audit team asked if we should indicate that in the audit report. I said there were better ways to communicate the results of the audit and our assessment—as well as our advice and insight—than the formal, written audit report.

I sat down with the division CEO, one of the top three executives in the company, and shared the facts. He told me he had suspected a management problem but hesitated to act because the corporate chief financial officer (CFO) favored the department head. He asked what I thought should be done—I refrained from recommending specific actions, in the interest of maintaining my independence.

We issued the audit report after discussing the situation with all senior parties. In the report, audit committee members saw an assessment that, while errors had been made, appropriate actions had been taken. I shared the rest of the story with them at the next audit committee meeting, with additional comments from the division CEO and the corporate CFO.

Was this an act of bravery? Looking back, I can say that while it was difficult to tell senior management that a rising star was not only underperforming but unlikely to be effective in the future, the risk to me was minimal. I explained the facts objectively and dispassionately, allowing senior management to make an informed and intelligent decision. They respected that ability and our willingness to go beyond traditional

Confronting peers on inappropriate interpersonal behavior happens less than **50%** of the time in organizations, according to the 2018 Workplace Courage Acts Index.

WHAT IS BRAVERY?

Under ideal circumstances, the audit committee would help create an environment that enables the chief audit executive to be brave. But few board members will oppose an angry CEO or CFO in favor of a respected but more junior and expendable executive.

Internal auditors need to be brave, but not reckless. Several practices can help auditors take bold action when needed, including:

» Building trusted relationships with the top executives and each individual on the audit committee.

» Planning the communication carefully, laying the groundwork for each discussion. Make sure your words are clear and unlikely to be misunderstood.

» Communicating in person, one-on-one, and not relying on others to communicate for you.

» Moving progressively up the organizational hierarchy, approaching each individual with an open mind and listening to his or her views – obtaining agreement and support before moving to the next level. Respect each individual's needs and the implications of the situation for him or her personally as well as for the organization. Consider asking each of them to attend your meetings with more senior management, all the way to the board, as appropriate.

» Listening and being prepared to modify your assessment if you're wrong, even if it's just moderating the language.

» Talking with and listening to allies and others who can help you.

» Ensuring no one is surprised, especially in front of others.

» Building a reputation for maintaining professional integrity. Honesty, ethics, and professional responsibility should always be top of mind.

auditing to provide them with our insights on the management of Commercial Accounting. By the time I had to report to the audit committee, I had the support of each member of management. The division CEO, who attended the meeting, told the directors he agreed with our assessment and that we had taken the appropriate action.

THE FEARFUL CAE

At my next company, the audit team uncovered financial statement frauds in several U.S. locations within the organization's largest business unit. The company had more than 100 locations around the world, most of which were underperforming. Senior management was thinking about consolidating operations to cut costs, placing the locations' general and financial managers under great pressure.

I wanted to know why so many local U.S. controllers were manipulating their financial results to show profits when, in fact, they were breaking even at best. Our inquiries revealed they were not doing so to put money in their pockets; their motive was to save their unit from closure. But we also uncovered a more significant problem: When the local controllers reported a projected loss to the business unit controller at headquarters (HQ) during their quarterly updates, he consistently asked them to "find a way to make the number." After discussing the instruction with their local general manager and finding no legitimate means of achieving their financial targets, the unit controllers fabricated profits.

Once we started auditing, the frauds were easy to find — management subsequently terminated both the local controllers and general managers. But my concern was not limited to whether the business unit controller had acted inappropriately; I also considered the possibility of a pervasive control environment or culture issue.

The HQ business unit controller did not direct the unit controllers to act

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

inappropriately, but he failed to impress on them the need to act with integrity despite the pressure. When I explained the situation to the corporate CFO, to whom I reported, he expressed confidence in financial management of the business unit at HQ. I had no persuasive evidence that either the CFO or the HQ controller intended the units to manipulate their financial results. I asked the CFO to reinforce the need for integrity by sending a memo to that effect to the company's entire financial staff, but he said the code of ethics already covered this principle. I suggested a conference call with global finance leadership, but he said that was also unnecessary. I also suggested it might be prudent to have the local controllers report directly to HQ and then to him; he told me that was not how the organization operated.

"I learned that courage was not the absence of fear, but the triumph over it. The brave man is not he who does not feel afraid, but he who conquers that fear." —Nelson Mandela

After completing our investigations, we concluded the frauds were not material to the financial statements. Still, the underlying conditions had not changed, and the possibility remained that additional fraud might be committed. I felt an obligation to share the facts with our audit committee, as well as my belief that the organization's overall control environment could be improved to help the local controllers do the right thing regardless of pressure.

When I met with the committee chair, a retired CFO, he listened carefully and agreed that I had an obligation to share the facts, as well as my perspective on the control environment, with the full committee. He also agreed to talk to each of the audit committee members before the meeting to prepare them for the discussion.

Next, I informed the CFO that this would be on the audit committee's upcoming meeting agenda and outlined what I would say. I told him I would not imply he or his team was involved in the frauds. And while I offered to forewarn the company's CEO, the CFO insisted that I leave that conversation to him. The CFO also committed to share his perspective on the issue and what actions should be taken, after I had spoken.

Unfortunately, the committee meeting did not go well. The chair had not provided sufficient details about my report to all the committee members in advance, and one overreacted. He was afraid the CFO and corporate controller had been involved in the fraud, despite my assurance that I had no reason to believe they were. Although the committee member calmed down, the CFO did not speak up either to comment on the environment that led to the frauds or to suggest corrective actions. The CEO and the audit committee chair remained silent.

> Factors such as grit and proactive personality are predictive of greater social courage, according to “The Left Side of Courage,” published in a 2018 edition of *The Journal of Positive Psychology.*

After the meeting, I spoke with the audit committee chair again. He apologized for the way the meeting had gone but said the committee would not support me in a dispute with the CFO. He knew that the CFO had at one point asked me to stop the audits that were identifying the frauds, which I declined to do, and that our relationship was strained. Moreover, he was as surprised as I was that the CFO didn’t comment during the meeting and suspected that was deliberate.

The audit committee believed in me, but the CFO was also highly respected and “had a bigger business card.” Both the CFO and the CEO wanted this issue to “go away” without having to take action themselves.

Shortly afterward, the HQ controller reached out to me; he said I had acted with integrity, agreed with my perspectives, and gave me his support. Nonetheless, the CFO and I agreed a few months later that we should part ways, and I left the company some time afterward.

Was I brave? I knew the CFO did not want this “dirty laundry” aired before the audit committee, and I knew he would likely find a way to remove me at some point. But I was professionally obliged to share the facts and what they meant with the audit committee. In hindsight, I should have spoken to each of the audit committee members myself, despite the chair saying he wanted to do it. Nobody attending the audit committee meeting should have been taken by surprise, as one director clearly was.

Perhaps others, such as the CAE I mentioned earlier, would have been more prudent. But even with hindsight, I believe I did what I had to do.

TAKE A STAND

Internal auditors must be determined to tell the harsh truth and do so in a way that clearly explains the facts and any recommended actions. They need to be prepared to sacrifice their job, and even their career, if necessary. Auditors must be brave, acting in the best interests of the organization and consistent with their principles. Anything less is a disservice to the profession and the stakeholders we serve.

NORMAN MARKS, CRMA, CPA, *was a CAE and chief risk officer at major global corporations for more than 20 years.*

Justin Pawlowski
Marc Eulerich

As important as it is, internal auditing involves a lot of repetitive work to provide assurance and achieve the department's objectives. There is supporting evidence to request, data to gather, workpaper templates to create, and controls to test. But imagine if these basic tasks could be automated.

That is the promise of robotic process automation (RPA). Many internal audit functions are looking to RPA to multiply the capacity of their teams. These departments are following the lead of the growing number of organizations that are using robots, or bots, to automate business processes – particularly repetitive and often time-consuming process steps.

RPA can help streamline processes by making them more efficient and more robust against errors. That may be one reason that 40% of internal auditors reported that their organizations currently use RPA in business operations in a poll taken during The IIA's 2019 International Conference in Anaheim, Calif.

Audit functions can catch up with their organizations' use of RPA by deploying bots as a digital workforce to enhance their assurance capabilities. Moreover, RPA can free internal audit's experts from the drudgery of repetitive activities to focus on critical thinking tasks and managing exceptions.

WHAT'S IN A BOT?

RPA involves software that autonomously executes a predefined chain of steps in digital systems, under human management. Common capabilities of bots include filling in forms, making calculations, reading and writing to databases, gathering data from web browsers, and connecting to automated programming interfaces. They also can apply different logical rules such as "if, then, else" or "do while." And those bots don't sleep, tire, forget, complain, or quit.

With RPA, bots improve over time as people specify the underlying rules, but they cannot learn on their own. Conversely, cognitive automation learns and improves its own algorithms over time based on the given data and experience.

RPA solutions can deliver benefits such as:

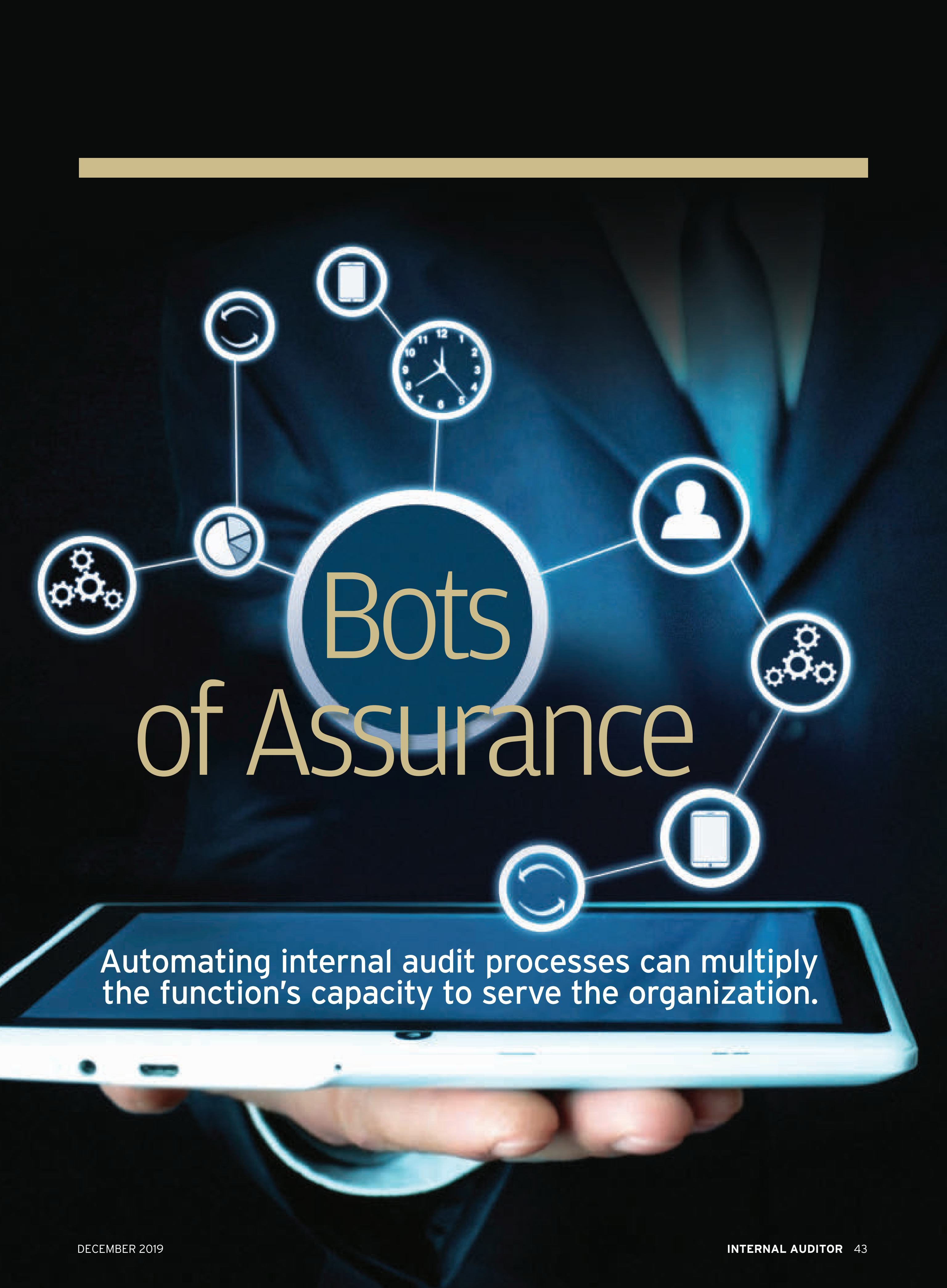
- » Increased efficiency, especially in situations that once involved repetitive and recurring manual work processes.
- » Increased effectiveness and robustness of processes that previously were prone to high error rates.

Organizations are most likely to realize these benefits when they use structured data, which provides the predefined instructions bots need to handle work scenarios.

FIVE TYPES OF USES

Internal audit departments may be slower than their organizations, as a whole, to deploy RPA, but there are many ways they can put the technology to use. Although these applications may differ, depending on each department's circumstances and

ANDRANIK HAKOBYAN / ISTOCK.COM

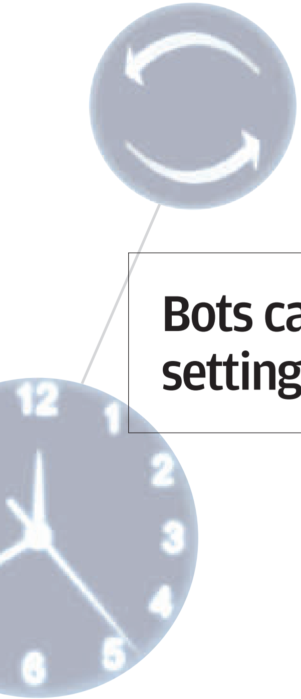


Bots of Assurance

Automating internal audit processes can multiply the function's capacity to serve the organization.

capabilities, they can be classified into five categories.

Support This category of applications enables internal auditors to perform or document an audit procedure such as creating workpaper templates. One example of a support application is a bot that downloads attachments. Internal auditors spend a lot of time pulling supporting evidence from electronic sources or waiting for audit clients to do so manually. In a typical enterprise resource planning (ERP) system, auditors may need to take as many as 10 steps to access an electronic attachment. These steps include opening the ERP browser, typing the transaction code, entering the document number and company code, adding the fiscal year, going to the attachments, choosing the correct file path, and entering a file name that complies with a predefined structure.



Bots can quickly identify inappropriate settings organizationwide.

A downloading attachment bot supports internal auditors by pulling electronic attachments automatically and more quickly—in less than 10 seconds per transaction. This can accelerate audit procedures related to vendor invoices, for example. In this context, the bot can support auditors in reviewing potential duplicate payments not yet returned, invoice approvals that are not workflow based, and invoice verification as part of a purchase-to-pay process audit. “Bot Programming” on page 45 describes how auditors can use rules to set up a bot.

Validation Bots in this category validate the accuracy or completeness of transactions under review. An example is a distance bot that validates mileage allowances for a full population of business trips, rather than by sampling. To calculate the distance between the starting point and destination manually using a geographical map service would take up to five steps. These steps include opening the web browser, typing in the starting point and destination address, and copying the distance displayed before continuing with the next distance.

The distance bot supports internal auditors by pulling as-is distances from the system automatically. This bot is good for performing travel expense audits, particularly in organizations with high expenses from mileage allowances.

Control Testing This category of bots performs all or selected testing steps or attributes for internal controls, especially for IT application controls and IT general controls. Organizations often have a clear picture of the “to be” status of these controls. By translating this clear picture into rule-based procedures, auditors can program bots to test both the design and operating effectiveness of such controls. Bots can quickly identify inappropriate settings organizationwide. For example, within a purchase-to-process audit, bots can test IT application controls such as the duplicate-invoice check and the three-way-match, and prepare standardized audit evidence.

Data Generation For internal audits requiring access to extended data sets, bots in the data generation category provide access to new data sources such as electronic attachments and temporary data sets. Data extraction bots support upgraded analytics and can reduce false positives by considering new data sources. This capability can reduce follow-up activities for false positives while increasing efficiency. For example, these bots can extract data from PDF text in less than one

RPA can improve compliance, quality, accuracy, and productivity, as well as reduce costs, notes Moving Internal Audit Deeper Into the Digital Age: Part 1 from the Internal Audit Foundation and Deloitte.

BOT PROGRAMMING

When setting up a bot, auditors not only must list the different processing steps, but also state how to get from one step to the next. For example, to access an electronic attachment, from the step where the ERP browser is opened, auditors instruct a bot to type in the transaction code, followed by pressing "enter." The bot follows the same process as a human user to enter the document number, company code, and fiscal year. Each of the first two entries is followed by pressing "tab." The third entry is followed by pressing "execute."

From there, the bot clicks the attachment button, followed by clicking "Attachment List," and double-clicking on the attachment file. Auditors specify a predefined valid file path for the bot to follow. Then, they instruct the bot to enter the file name and click "save." Putting these steps into a loop sequence directs the bot to go through the activities over and over for each document specified in the source listing.

second and from image files in less than three seconds.

Reporting Auditors can use bots in this category to create reports or operate follow-up procedures. If internal audit does not use specialty audit software—or plan to introduce it—bots can automate repetitive activities such as report creation based on an audit program and sending follow-up reminders and inquiries.

PLAN FOR THE PITFALLS

The previous examples demonstrate how bots can enable the internal audit function to accomplish results more quickly and without human errors. While the improvements may outweigh the implementation costs, internal audit should be aware of risks across three dimensions: operations, reporting, and compliance. Internal auditors should manage these risks from the beginning and throughout the implementation of RPA. They should start by addressing some common pitfalls.

Disregarding Other Automation Possibilities Do not automate audit procedures with RPA when other affordable software or more advantageous automation possibilities are available. For example, specialty audit software may be used for reporting and follow-up activities.

Outsourcing Full Bot Programming RPA bots can be improved over time as auditors specify rule-based procedures to reduce the number of false positives and false negatives. Outsourcing this programming can make internal audit dependent on a third party to establish the logic followed by each bot. Instead, internal audit should obtain advice from external parties, if needed, while keeping most bot programming in-house.

Complying With the RPA Tool's Terms of Use Software license terms may prevent internal audit from taking an existing RPA tool used in selected subsidiaries and using it for organizationwide audits. Typically, the license is for the licensee's (subsidiary's) direct business purposes—not for all affiliates across the organization. Examine the terms of use carefully.

STARTING WITH BOTS

Knowledge of RPA's benefits and risks can prepare internal audit to explore the technology's potential. These tips can help internal audit get started.

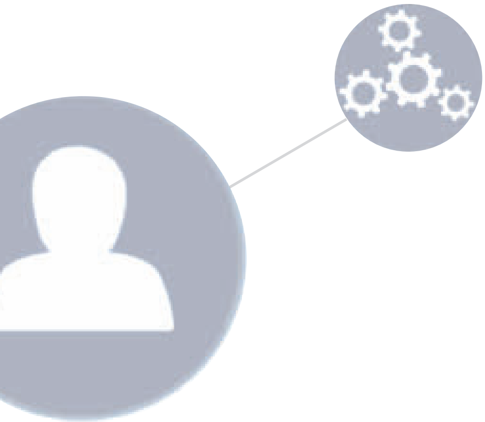
Identify Use Cases Auditors should begin by identifying their department's

VISIT OUR MOBILE APP + InternalAuditor.org to watch a video on robotic process automation.

recurring activities. Where is time lost because of repetitive activities? Where does the department want to provide higher assurance by increasing sample sizes or extending substantive audit procedures? This identification exercise should be separate from the discussion about how to automate internal audit activities. It also may comprise both full and partial automation.

Internal audit can use workshops to identify automation opportunities. During these sessions, auditors can use a matrix to prioritize cases based on the potential benefits of automation and the feasibility of doing so. Mapping automation opportunities by end-to-end processes usually doesn't pay off. Instead, internal audit should map subprocesses or process variants because these are at an actionable level. However, not all subprocesses or variants are an opportunity for automation.

Internal audit should align RPA with its overall digital labor strategy.



In addition, internal audit should not create silos between different automation possibilities. When assessing use cases, internal audit should consider RPA as one alternative among many.

Assess the Internal RPA Landscape Because internal audit is not usually the early adopter for RPA within organizations, the department should identify tools and resources already in use. To realize RPA's full potential, auditors should assess the various tools on the market.

Instead of going on its own, internal audit can partner with the organization's existing RPA users to develop a pilot to demonstrate how RPA can be used in audits. Choosing a use case that allows internal audit to quantify its benefits can support internal discussions and decisions about using RPA.

Motivate the Internal Audit Team

The pilot's results and the possibilities of learning from RPA are two main drivers for motivating the internal audit team to apply the technology. Demonstrating learning opportunities is easy by using online tutorials, community forums, and free trial versions. These resources can provide online training and enable internal auditors to become familiar with RPA tools. Trial versions, in particular, can show auditors how easy it is to use the tool, which can motivate them to use it.

RPA IN ALIGNMENT

In addition to these three tips for getting started, internal audit should create an implementation plan and align RPA with its overall digital labor strategy. This plan should balance an understanding of the technology's risks with the benefits of target-oriented approaches to implementing it.

To realize RPA's benefits in the long run, internal audit should deploy it from a governance perspective. The board's support can especially enable the chief audit executive to develop a clear plan for automating different internal audit processes. Because other business functions may be using RPA, internal audit needs to align its RPA implantation with these existing activities to generate synergies and avoid duplication of efforts. That understanding can position internal audit to put RPA to use and also drive effective reviews of the organization's RPA program. Ia

JUSTIN PAWLOWSKI, CIA, CCSA, CRMA, *is chief audit executive at ALSO Holding AG in Emmen, Switzerland, and a 2015* Internal Auditor *Emerging Leader.* **MARC EULERICH** *is professor for internal auditing at University of Duisburg-Essen in Germany.*

An uncertain and volatile political landscape has created an opportunity for internal audit to help the organization prepare for the worst.

The Rise of Political Risk

Neil Hodge

Illustration by Sean Yates

It hasn't been a good year for Chinese tech giant Huawei. Last winter, the U.S. asked Canada to arrest the company's chief financial officer, Meng Wanzhou, on spying charges. By mid-May the U.K. government was embroiled in a fight about whether to allow the firm to be involved in developing the next generation of communications networks. Meanwhile, customers were starting to avoid Huawei's products after hearing that Google would no longer allow them to update some Android products, citing U.S. sanctions. The impacts are clear for Huawei, but many other firms were left asking what repercussions it could have on their contracts, markets, customers, and business decisions. How would China retaliate? What other businesses could be caught in the crossfire?

This is just one example of the questions that arise when even a small part of a business is caught up in a revolution or exposed to economic crises, coup d'états, interstate trade disputes, economic sanctions, or diplomatic clashes. Such risks ebb and flow with the diplomatic tide; however, as businesses become more dependent on international markets and extended supply chains, they are more exposed to political risks.

Risk management specialist Marsh, for example, highlighted a period of

BASE PHOTOGRAPH: KITTYVECTOR / SHUTTERSTOCK.COM

"Most organizations have still done very little to prepare for Brexit, despite knowing that the worst-case scenario of a 'no deal' option is very much on the table."

Michael Moore

"Organizations should be prepared for every scenario—worst, best, and everything in between."

Ian Stone

"unprecedented uncertainty" in its Political Risk Map 2019, citing a rise in geopolitical tensions (namely, Russia against the rest of the world) and protectionist sentiments (namely, the U.S. against the rest of the world).

Although companies with multinational operations or overseas supply chains have always had to review their exposure to political risks, most U.K.-focused businesses have added the topic to their risk registers only in the past few years. "Up until the election of Donald Trump in the U.S. and the vote for Brexit in the U.K., political risk was always something that companies in other countries had to think about," says Michael Moore, director general at British Private Equity and Venture Capital Association, former Liberal Democrat Member of Parliament, and the Secretary of State for Scotland who helped prepare for the 2014 Scottish independence referendum. "It never even registered that U.K. companies would need to consider their home country as being politically risky."

Worse still, he says, companies have been slow to react. Although Brexit has been a major political and corporate issue for the past three years, Moore says that most U.K. companies have not made any significant preparations for the country leaving the European Union. "Most organizations have still done very little to prepare for Brexit, despite knowing that the worst-case scenario of a 'no deal' option is very much on the table," he says. "It appears that businesses want more certainty about what the outcome is going to be, which rather flies in the face of planning for political risk." The U.K. has called for a general election on Dec. 12, 2019, and the EU has agreed to extend the Brexit deadline to Jan. 31, 2020.

It is possible to react quickly to changing circumstances only if all the parts of the business think the same way.

Brexit is, of course, just one of many political risks on the global map. Whether organizations are exposed to the fallout from a U.S. trade war with China or increased sanctions on Iran or North Korea, or are more worried about political instability in Venezuela, Russia's intentions in Ukraine, Chinese military strength in the South China Sea, war in Yemen, or the ever-present threat of terrorism worldwide, none of the current global political risks is likely to disappear soon—organizations need to know they can react rapidly to changing circumstances. Internal auditors should be able to provide assurance on this area and feature political risks in their audit plans.

RAPID RESPONSE

Ian Stone, CEO and founder of business advisory company Vuealta, says that he expects political uncertainty to remain one of the biggest challenges facing decision-makers for the next five years. He warns against trying to "predict the future." Instead, he advises them to focus on being fluid.

"Organizations should be prepared for every scenario—worst, best, and everything in between," he says. "Successful businesses can then choose their course based on the information they have and use the latest technology to test 'what-if' scenarios against those plans to cover all bases."

He adds that it is possible to react quickly to changing circumstances only if all the parts of the business think the same way and are aware of what they need to do in any given situation. "Planning can be vital in responding to an unpredictable political situation," he says. "No matter how big the organization, if all departments—from

Geopolitical instability is the No. 3 major emerging risk, with experts citing the decline in multilateralism and the rise of populism, according to 2019's AXA-Eurasia Group Future Risks Report.

sales and finance to marketing and the supply chain—are not connected, they will never keep pace with rapidly changing and volatile international markets. When one area of the business changes, the effects ripple across the whole company."

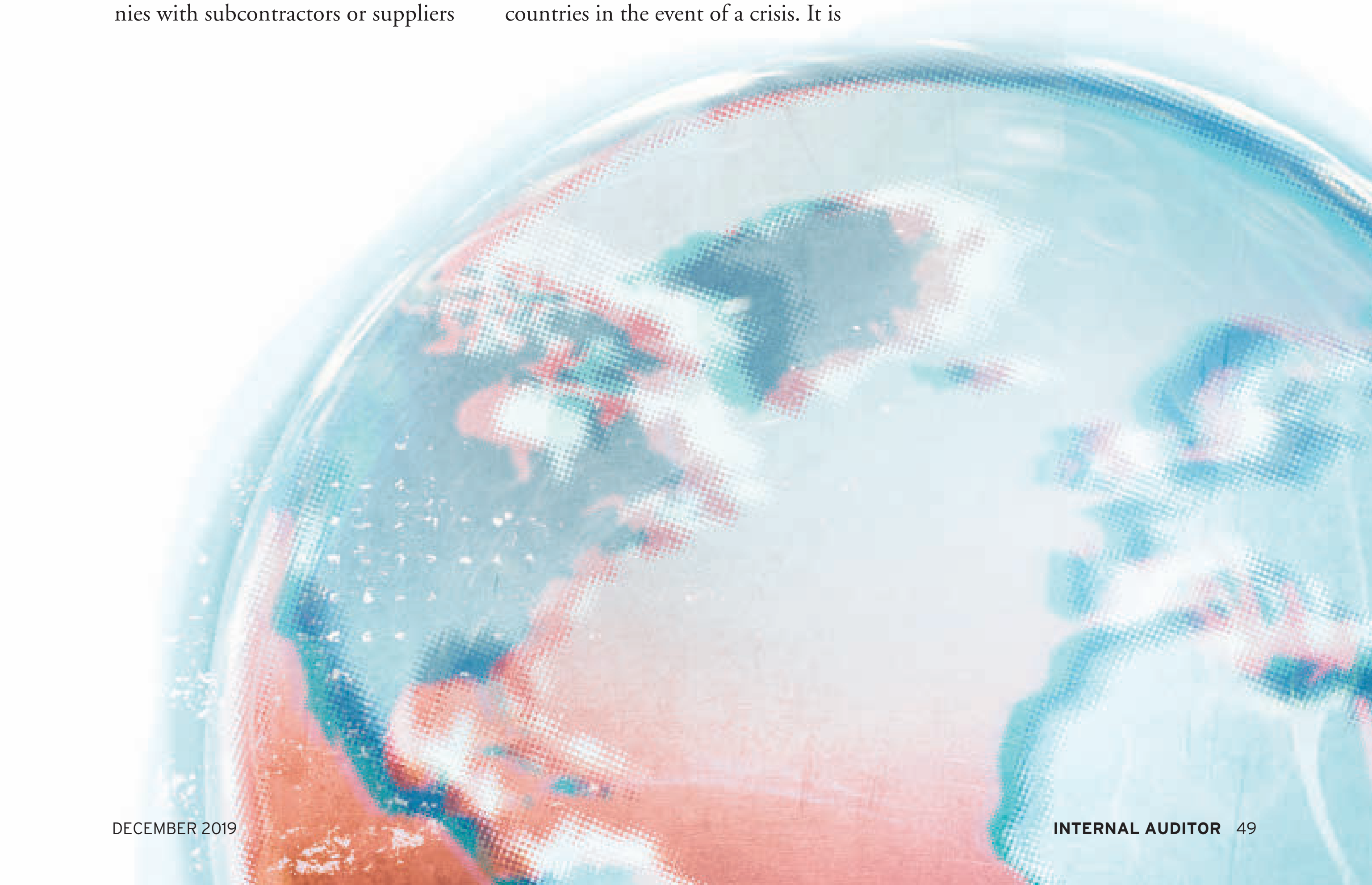
Business continuity is an obvious priority for those already accustomed to operating in a volatile political environment, so internal audit should review continuity plans regularly. Tom Tahany, an intelligence analyst at security firm Blackstone Consultancy, says it is vital to ensure all threats and risks that could interrupt the business' output are identified, and plans are up to date and effective. "You may need to prioritize the resilience of key functions so that these can continue, while business areas that are less immediately crucial are brought back online when possible," he says.

Conversely, however, companies with subcontractors or suppliers abroad, but with no direct presence overseas, also need to understand how their supply chains and customers could be affected by events outside of their control. It's generally wise not to rely too heavily on a small group of suppliers and to ensure they are not all in the same political region or subject to the same political forces. It's also important to keep monitoring changing circumstances and to think broadly about how political developments in one place could potentially have effects elsewhere.

"You cannot prepare for every possible eventuality and plan a response for every minutia in a crisis," Tahany says. In some ways this is a good thing. It allows companies a degree of flexibility in planning responses. However, you may need evacuation plans of varying magnitudes and secondary and tertiary options to help staff in different countries in the event of a crisis. It is

"You cannot prepare for every possible eventuality and plan a response for every minutia in a crisis."

Tom Tahany



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

important that companies are prepared for anything, rather than everything."

RELIABLE SOURCES

A key problem with political risk is that it can be difficult to get reliable, timely, and accurate information, especially if events unfold quickly—for example, in a government coup, revolution, riot, civil unrest, or an invasion. Another problem is how to quantify the impacts of these risks and assess what contingencies need to be taken and when.

If asked to provide assurance about operations in another country or region, internal auditors may find it helpful to talk to employees based there and look at risk indicators provided by global nongovernmental organizations, such as Freedom House, the International Monetary Fund, Transparency International, and the World Bank, whose opinions may provide a base layer for measuring risk. However, Pornprom Karnchanachari, a partner at Thailand-based law firm Legal Advisory Council, warns that some "on the ground" views can be skewed by poor reporting, inaccurate commentary, and information sources that cannot easily be challenged or verified. When Thailand experienced a coup in 2014, social media and news coverage helped to spread misconceptions of the political situation, making it seem extremely risky. However, the on-the-ground situation was quite different, he says. Foreign companies were not affected by the political changes, and business continued as usual under the existing legislation while political stability was restored. So, for example, he says, social media "should be taken with a pinch of salt."

"Companies need to look for the advantages that a change in political circumstances might afford."

Paul McIntosh

Internal audit can play a significant part in evaluating the level of risk and can offer an objective view.

More reliable sources of information include embassies, which "can offer a basic, but generic, overview," and local and foreign chambers of commerce, Karnchanachari says. But the best source is foreign companies that have been on the ground for some time, as they will have a government affairs team that can share useful insights.

"It is only by arming the business with various viewpoints and understanding the history, culture, and unique situation in each country that a business can build a robust understanding and approach to political risk exposure," he says. However, sometimes you need to act swiftly.

Ben Abbouddi, global threat analyst at travel and health-care risk management firm Healix International, says companies should always consider the worst-case scenario. A risk matrix that places the likelihood of a risk against its impact can help highlight the most significant risks and those that would require the most time and resources to manage. It may also help to eliminate political "red herrings" that attract media attention, but do not have a significant impact.

Internal audit can play a significant part in evaluating the level of risk and can offer an objective view if there are clashes of opinion. For instance, project managers working in some regions may find themselves at odds with risk managers at the headquarters office. Their perception of local risk may be very different, and their incentives could make them anxious to pursue contracts or business that, correctly or incorrectly, are seen to be high risk.

LEVEL-HEADED ASSURANCE

Jack Darbyshire, manager at De-Risk, a strategic risk management planning

There has been a 150% increase in the number of countries using social media manipulation campaigns in the last two years, according to The Global Disinformation Disorder from the University of Oxford.

firm, says internal audit teams can assess whether risk managers are being too cautious about particular regions. "Uncertain times can make risk managers focus on risks that will probably never happen," he says. "Risk management is a negative concept, and many traditional risk management teams think so negatively that they end up worrying about extremely unlikely scenarios. This may make project managers reluctant to share communication with the team."

This is another reason why accurate, timely, and trustworthy information is vital. Organizations could lose far more than they gain by failing to do profitable business, implementing emergency plans unnecessarily, and removing staff or closing operations, only to find that the crisis blows over. Internal auditors should assess the quality and quantity of information available to management while it makes such difficult decisions. Internal auditors also could consider whether there are other sources of assurance available.

LOOK FOR OPPORTUNITY

A political crisis may also bring opportunities. Paul McIntosh, CEO of Bridgehead Agency, points out that it is equally important that organizations consider potential advantages associated with volatility. "Companies need to look for the advantages that a change in political circumstances might afford, and not just think about the risks," he says.

Brexit is a case in point. "No matter what kind of deal — if any — the U.K. gets, the E.U. and the U.K. are likely to remain major markets, and companies want to continue to do business in both," McIntosh says. "If there is more paperwork in the future, it will add to costs, but this is usually not as difficult or as expensive as some think. Whichever way you look at it, Brexit will create opportunities — possibly not as many as staying in a single market — but companies need to explore these and exploit them."

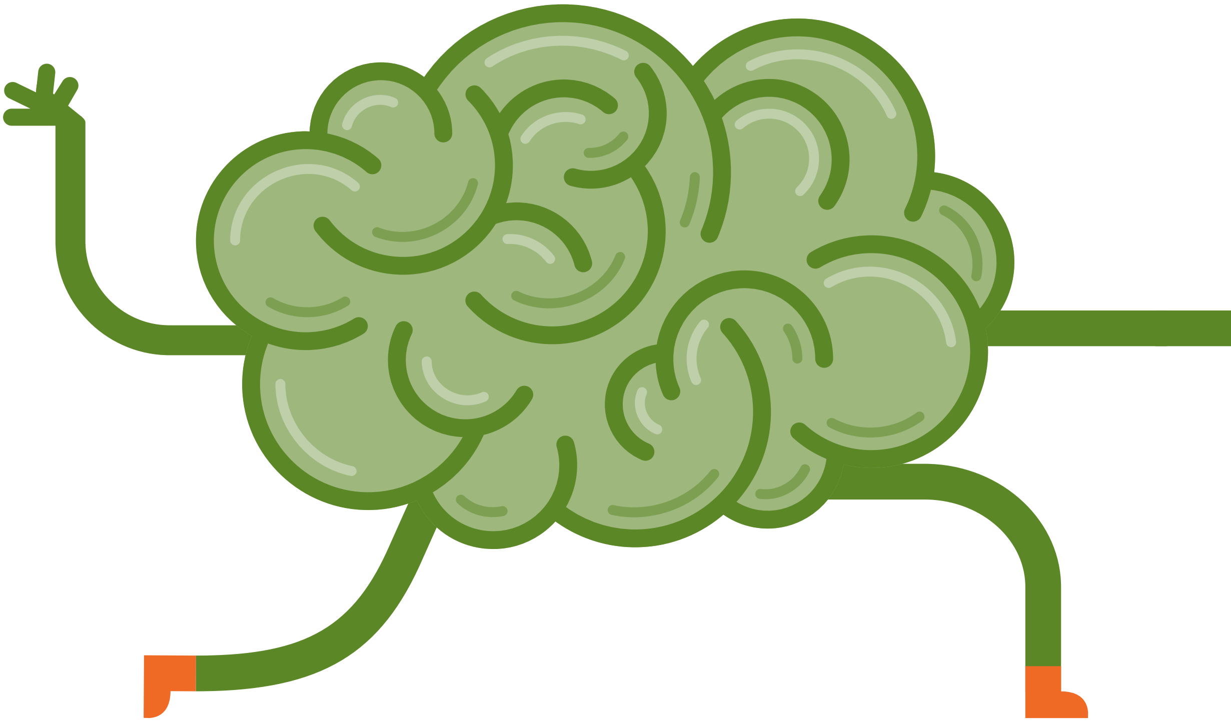
NEIL HODGE *is a freelance journalist based in Nottingham, U.K.*

A version of this article first appeared in the July/August 2019 issue of Audit & Risk, *the magazine of the Chartered Institute of Internal Auditors. Adapted with permission.*

STATEMENT OF OWNERSHIP, MANAGEMENT, & CIRCULATION

Extent and Nature of Circulation	**Average No. Copies** (October 2018-August 2019)	**Actual No. Copies** (August 2019)
Total Number of Copies	73,480	70,369
Paid Circulation Mailed Outside-County Paid Subscription	56,731	54,847
Paid Distribution Outside the Mails Including Sales, Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS	14,559	14,058
Total Paid Distribution	71,290	68,905
Free or Nominal Rate Copies Mailed at Other Classes Through the USPS	56	57
Free or Nominal Rate Distribution Outside the Mail (*Carriers or other means*)	648	642
Total Free or Nominal Rate Distribution	704	699
Total Distribution	71,994	69,604
Copies Not Distributed	752	775
Total	72,746	70,379
Percent Paid	99.02%	99.00%
Paid Electronic Copies	17	19
Total Paid Print Copies + Paid Electronic Copies	71,307	68,924
Total Print Distribution + Paid Electronic Copies	72,011	69,623
Percent Paid - Both Print & Electronic Copies	99.02%	99.00%

Publication Title: *Internal Auditor*
Publication Number: 0020-5745
Filing Date: 9-27-19
Issue Frequency: Bi-monthly
Number of Issues Published Annually: 6
Annual Subscription Price: $75.00
Mailing Address of Known Office of Publication: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, Seminole County,FL 32746
Address of Headquarters: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Contact Person: Gretchen Gorfine Telephone: 407-937-1232
Publisher: Monica Griffin, CMO, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Editor: Anne Millage, Editor-in-chief, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Managing Editor: David Salierno, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Owner: The Institute of Internal Auditors, Inc., 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746
Issue Date for Circulation Data: October 2018 - August 2019 / August 2019
Signature and Title: Gretchen Gorfine, Production Manager, 9-27-19



PLATERESCA / ISTOCK.COM

The need for internal auditors to understand and apply critical thinking seems self-evident, especially with research showing the importance chief audit executives (CAEs) place on this skill. It's also made an outstanding showing in The IIA's annual Pulse of Internal Audit survey over the years. In 2018, 95% considered critical-thinking skills essential to their function's ability to perform its responsibilities.

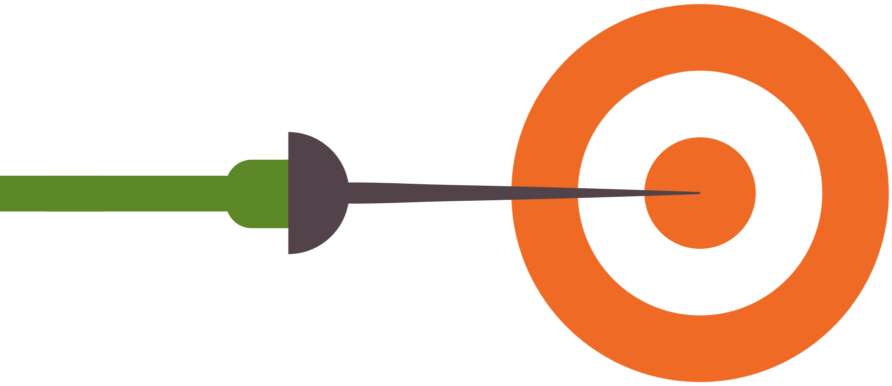
Unfortunately, while everyone agrees that critical thinking is important, they find it hard to define exactly what it is. If you ask 10 CAEs, you are likely to get 10 different answers. And at the core, those answers boil down to nothing more than internal auditors using their brains.

Fortunately, The Foundation for Critical Thinking provides a more practical definition: "The intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action."

Using this definition, the Foundation for Critical Thinking developed an outline for critical thinking based on eight elements, described in the book, *The Thinker's Guide to Analytic Thinking,* by Linda Elder and Richard Paul. Following is a framework for internal auditors' use of critical thinking based on these elements.

By following a critical-thinking framework, internal auditors can better hone this sought-after skill.

J. Michael Jacka



Use your head

THINKING CRITICALLY

Critical thinking requires understanding the purpose of the individual task toward determining the question to be answered. It also involves recognizing the various points of view brought to the task, as well as the assumptions, concepts, and theories upon which the work will be based. Information is gathered, leading to inferences or preliminary conclusions, which come together to provide final conclusions and consequences.

Thinking critically about the audit process means thinking critically about audit engagement tasks. This requires evaluating the tasks, such as interviews, functional tests, and risk assessments to better understand not only how they are completed, but also how critical thinking was used and how it can be used more effectively in the future. Some people consider critical thinking to be "thinking about how you think."

Understand the Purpose Identifying the objective of an audit engagement is fundamental. But the first step in critical thinking applies this concept to each activity conducted within the audit, providing guidance for the critical thinking that follows. The objective of an interview might be to learn the interviewee's understanding of the process, the purpose of a test might be to ensure the organization is compliant with a specific regulation, and the goal

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

of a meeting might be to confirm all parties understand the audit process. These objectives are often assumed, but critical thinking requires the auditor to be able to articulate them.

Determine the Question The point of critical thinking is to come to a conclusion regarding a question or problem. Therefore, to think critically, internal auditors need to determine, based on the previously defined purpose, what question the individual task (test, interview, process documentation, etc.) will answer. Does this person understand his or her role in the accounts payable process? Is there a more efficient way to ensure new hires are appropriately vetted? Does the data support the effectiveness of controls? The question can be specific or broad, based on the detail of the work being done and the individuals involved. But it should align with the task's purpose, as well as the overall purpose of the engagement.

Understand Your Points of View Everyone approaches a situation with points of view, both positive and negative. Effective critical thinking requires understanding how they impact the ensuing analysis. Internal audit's point of view might be that the department helps the organization achieve its objectives. However, because of internal audit's focus on risks and controls, it also may approach engagements with a point of view that is skewed toward risk aversion or ignores missed opportunities as part of an assessment. For this reason, it is important to also consider other points of view and, as appropriate, include them in the analysis.

At the core of critical thinking is information, which is the lifeblood of internal audit work.

Determine Assumptions Effective critical thinkers step back to determine the assumptions—beliefs we take for granted at subconscious or unconscious levels—being made to adjust for them. These can be positive (everyone in the organization is working toward success, or the client sees internal audit as a partner) or negative (the department being reviewed has never run well and will continue to run poorly, or no one in the organization sees the value of internal audit). Any of these could be true, but they should be evaluated to determine if they are accurate and what impact they will have on the analysis.

Identify Concepts and Theories Concepts, theories, and principles help make sense of things. They are different than assumptions, which are ideas and beliefs brought to a project. Concepts and theories are the additional information and ideas that may be needed to conduct the analysis. Some of this information may already be known, such as control frameworks or standards for internal auditing. Others may require additional research, such as applicable laws and regulations or best practices in the industry. Ultimately, the internal auditor should confirm that, in every audit task, he or she understands the concepts and theories needed to answer the question being asked.

Gather Information At the core of critical thinking is information, which is the lifeblood of internal audit work. Without it—data, evidence, and facts—there is nothing on which to base inferences and conclusions. Information should be applicable to the purpose and the question being asked, and the points of view, assumptions, concepts, and theories can result in the need for additional information. Many

Critical thinking is the No. 2 skill most in demand by CAEs and internal audit professionals, according to Protiviti and ISACA's 2019 Global IT Audit Benchmarking Study.

audit processes—interviewing, testing, process analysis, etc.—also are methods for gathering information.

Recognize Inferences Analysis should begin when the audit engagement starts, with the auditor immediately drawing inferences and preliminary conclusions. This involves constructing hypotheses regarding what is occurring, then subjecting them to further analysis. For example, an initial interview may infer that a process is well-understood and controls are effective. Subsequent testing proves that controls are not working as designed and significant delays and errors are occurring. It is not that the initial inference was incorrect. Rather, the initial inference provided a base to identify the need for additional information.

Provide Final Conclusions and Consequences This is the final step in the critical-thinking process. The testing, interviewing, reviewing, and analyzing lead to conclusions that answer the question and satisfy the purpose of the audit task. The conclusions also should provide direction on how to proceed—more testing, more interviews, additional data gathering, or completing the audit engagement.

THE AUDIT PROCESS

The preceding descriptions show how every stage of an audit engagement can be evaluated with an eye toward using effective critical thinking. However, specific issues related to the elements of critical thinking should be considered within every audit task.

Risk Assessment One cause of the Great Recession was the subprime mortgage crisis. Analysts believe the complicated nature of these securities resulted in few people understanding how they actually worked or the impact of the associated risks. The lesson is that sufficient information should be gathered in the risk assessment process to ensure the intricacies of the process, as well as the associated risks, are understood. If the auditor does not feel comfortable with his or her understanding of how things work and how they might go wrong, then the audit task should not proceed until more information is obtained.

> **When a process or product is succeeding, the unconscious assumption is that risks are well-controlled.**

The subprime mortgage crisis also points to another important part of critical thinking in the risk assessment process: One reason the crisis was allowed to escalate was that everyone was benefiting. And people seldom question success. When a process or product is succeeding, the unconscious assumption is that risks are well-controlled. This leads to the inference that risks are mitigated and no further reviews are needed. Stated this way, we can see the fallacy. But it only becomes obvious when viewed through the lens of the critical-thinking framework.

Interviewing A good interviewer confirms the answers given answer the questions asked and support the overall purpose of the interview. In addition, because people, even internal auditors, have personal agendas, the interviewer should safeguard that no assumptions about the validity of answers intrude on inferences being drawn.

Inferences will be made during the interview regarding how new information may have changed the structure of the interview, the subsequent information gathering, the purpose of the interview, and, in rare cases, the purpose of

Critical thinking is a skill in high demand because it cannot be replicated by software or handed over to algorithms, says the European Confederation of Institutes of Internal Auditing's Risk in Focus 2020.

the engagement. Navigational change can come from any task within the audit process.

Process Documentation As with interviewing, information gathered during process documentation may result in navigational changes. And it is important that the internal auditor not look only at what is presented. Taking off the blinders—watching what else is occurring—may result in inferences and preliminary conclusions that change the focus of the audit. For example, if the auditor is working in a warehouse and notices an unmarked van occasionally picking up a box or two, it may represent a significant issue requiring follow-up. Even something as simple as a large pile of papers on a desk may indicate an issue that needs to be addressed.

Testing Entrepreneur and author Seth Godin notes, "Connecting the dots … is more essential than ever before. Why, then, do we spend so much time collecting dots instead? [A] big bag of dots isn't worth nearly as much as [a] handful of insight." The volume and accessibility of data has resulted in including as much data as possible in every test. Critical thinking requires understanding why specific data is needed—how it supports the purpose of the test, itself, and of the audit engagement. A 100% sample may not be required, no matter how easy it is to retrieve. Being awash in data can actually inhibit the critical-thinking process. Never gather data just because you can; gather data because it supports what you are trying to achieve.

REPORT WRITING

Much of internal audit's focus on critical thinking centers on report writing, when all the inferences and conclusions come together for presentation to the client. But everything that goes into the report—the data gathering, the process descriptions, the conclusions—should have occurred long before the report is drafted. If critical thinking is applied throughout the internal audit process, one of the biggest struggles in report writing can be eliminated.

The overall purpose of report writing needs to be understood and some additional questions need to be addressed, such as what is the purpose of the report, who is the report for, what does the reader care about, and what is internal audit trying to say? Answering these questions—reviewing the assumptions that are being made about reports—will give the internal auditor a better grasp of the content to include.

THINKING ABOUT HOW YOU THINK

Thinking about how you think is the first step every internal auditor should take. A good exercise is to take a specific task—an upcoming interview, functional test, or walk-through—and work through the critical-thinking framework. This will help auditors see the good and bad habits they use in the thinking process and allow them to build on their strengths and work on their weaknesses. Continue this exercise and, eventually, an increased awareness of how critical thinking is used in all situations will develop. And it will make auditors, audit departments, and the profession better.

> **Never gather data just because you can; gather data because it supports what you are trying to achieve.**

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

BY MATT KELLY

A NEW TOOL FOR DIRECTORS

The Guiding Principles of Corporate Governance are designed to help boards do better.

STEVE ALBRECHT

TAYLOR SIMONTON

LARRY HARRINGTON

The dictionary defines *principle* as a fundamental truth that serves as the foundation for a larger system of belief or behavior—a sturdy, versatile thing that, when used correctly, can address a wide range of issues. So it's welcome news that The IIA and the Neel Corporate Governance Center at the University of Tennessee in Knoxville have developed a set of Guiding Principles of Corporate Governance. After all, corporations have a lot of issues that need addressing.

Shareholders want better returns, even as they preach about long-term stability over short-term results. Regulators want compliance with standards for financial reporting, cybersecurity, business conduct, sanctions, and more. Consumers want low prices, prompt service, and environmentally friendly products, or else they'll flay the company on social media. Employees want a raise and a viable career path, or else they'll quit.

Those are a lot of constituencies and demands that corporations have to juggle somehow, with a heap of legal liability if boards steer the organization wrong. So, yes, sound principles of corporate governance are a vital tool for directors to have.

"It's not like you can read a book and then say, 'Oh yeah, I know exactly what my corporate governance should look like,'" says Steve Albrecht, a longtime business professor at Brigham Young University and elsewhere who has served on the boards of SkyWest Airlines, Cypress Semiconductor, and numerous other public and private companies over the years. He sees the governance principles as a mechanism to help boards hold themselves and their organizations accountable to the various objectives (financial, operational, legal, ethical) they might have.

Sure, companies also can be held accountable by law enforcement, activist investors, or social media campaigns—but if matters have reached that point, the board is already losing. "All those ways to hold corporations accountable are from the outside, except for corporate governance, which is from the inside," Albrecht says. "And they all have negative consequences except for corporate governance." In other words, good corporate governance is about an organization's self-discipline before outsiders decide to intervene.

What Governance Principles Entail

The Guiding Principles of Corporate Governance were developed to serve as a foundation for a new American Corporate Governance Index on U.S. publicly held companies released this month. The index is based on a survey of chief audit executives at an array of

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

U.S.-listed companies, creating a scorecard for overall corporate governance quality in the U.S.

The Guiding Principles reflect a compendium of viewpoints on corporate governance from sources ranging from the National Association of Corporate Directors, New York Stock Exchange, and Organisation for Economic Co-operation and Development to the Business Roundtable, The Committee of Sponsoring Organizations of the Treadway Commission, and the King Commission. Read through the nine points of the Guiding Principles, and a few themes emerge.

First, these principles are meant to establish durable practices—the muscle memory directors can use to guide their thinking, as they confront one issue after another. For example, Principle 3 talks about identifying key stakeholders and soliciting their feedback to make sure the organization's policies meet stakeholders' expectations. That's a practice boards need to be able to perform whether they're deciding on share buyback plans versus new investment (What do shareholders want right now? What will keep us competitive in five years?) or resolving dilemmas about ethical sourcing (Will our reputation among consumers be worth higher supply chain costs?).

Or consider Principle 6, that boards oversee the corporate culture of the business, assess the integrity of senior management, and intervene when culture and objectives are misaligned. As we keep moving into a more transparent world, where everything is available for all observers to see and dissect all the time, the alignment of values among a corporation and its stakeholders will matter more.

It won't suffice simply to declare your ethical values and culture of integrity.

It won't suffice simply to declare your ethical values and culture of integrity; even Enron did that. Organizations will need to demonstrate their embrace of those things in a visible way. The board bears ultimate responsibility for that, and Principle 6 reminds directors to keep that duty top of mind.

"There are a lot of things boards have to do," says Taylor Simonton, currently audit committee chair for Master Chemical Corp., Advanced Emissions Solutions, and Surna. "If they don't already have principles in place … some things can get missed."

Second, the principles also define how the board should govern itself. Principle 4, for example, lists eight criteria about directors' commitment of time, evaluation of performance, director education, meeting in executive session, and even compensation structure. Call all of that guidance about how a board can keep itself in trim and healthy shape, so it can execute all those duties mentioned above or in some of the other principles.

Putting the Principles to Work

OK, let's say the board has read the principles and likes what it sees. How would directors go about putting the principles to good use?

One idea is to review the board committee charters and assess how well they capture the spirit of the Guiding Principles. For example, the principles stress the importance of directors devoting sufficient time to their duties, meeting in executive session, and rotating directors as needed to ensure the right balance of institutional knowledge and new perspective. All good points. So how do the board's charters translate those points into specific requirements for attendance, training, meetings without the CEO present, or limits on committee tenure?

More broadly, the Guiding Principles also can help a board hone its thinking about what committees it should have (beyond those required by law). The principles stress the importance of identifying key stakeholders and monitoring key risks—but those things vary from one company to the next. So can the board articulate why it does or doesn't have, say, an IT risk committee, or a public policy committee?

Every board would *like* to say yes, it can; but the Guiding Principles make it much easier for a board to say, "We started by measuring ourselves against the principles, and reached these decisions, which explain why our board is structured the way it is."

Larry Harrington, former head of internal audit for Raytheon and a past chairman of the board of The IIA, sees the Guiding Principles as a maturity model. Boards can use the principles to plot their location on that model, and map out steps for improvement.

That idea of a maturity model raises an important point: A board must *want* to improve to take full advantage of the principles. Otherwise, the principles are just more window dressing, like Enron's fabulous code of conduct. "The folks who really need the guidance don't pay any attention to it, and the folks who generally do a good job use it as a barometer for 'What else can I do better?'" Harrington says. "Because they do want to do better." Ia

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

INTERNAL AUDITING IN 2020

The IIA's Global and North American Board chairs consider the opportunities facing the profession in the coming year.

MIKE JOYCE
Chair
IIA Global Board
of Directors

BENITO YBARRA
Chair
IIA North American
Board of Directors

What are the biggest risks organizations will face next year?

JOYCE For many, cybersecurity, data management, and third-party vendor compliance will remain the biggest immediate concerns. Recruitment and retention of skilled employees will be an ongoing challenge. However, we are living in an unusually high period of general uncertainty. The economic and political environments, extreme weather, trade relations, regional military action, etc., all create the potential for "black swan" type risk events that auditors should be thinking about. This may require revising traditional risk assessment approaches to reflect the potential impact of these uncontrollable events.

YBARRA The continual rise of automation, robotics, and the less-than-predictable geopolitical climate will impact how organizations do business and will challenge their resilience. There will be more pressure to ensure operating strategies and staff are agile and flexible enough to withstand a potential recession, impacts to supply chains, and a changing workforce. The talent and platforms that are creating value today may need to quickly shift and adapt as things change more rapidly.

What risks do digital transformation initiatives present organizations?

YBARRA Organizations must ensure that digital transformation initiatives are prioritized and measured based on the criticality of their data assets. Undisciplined approaches that do not consider classification, access, and data security could incur more costs than the transformation is projected to save. Ensuring key players are involved in the development and execution of initiatives is critical to achieving higher success rates.

JOYCE The first risk would be failing to recognize the need to transform one's business model quickly enough, and to establish a clear vision of the desired end state. The second risk would be failing to effectively manage these projects. These transformative projects tend to exceed expectations regarding complexity, budget, resource demands on personnel, scope creep, etc. Equally vital is ensuring a flawed process is not digitized in the hope that greater use of technology alone will create value. Like most large projects, a digital transformation initiative requires clearly established objectives that support the stated strategy, adequate resources and support from senior management, continuous supervision, measurable metrics to gauge progress, and contingency and parallel operational capabilities to mitigate delays.

What opportunities does the recent change to the Statement on the Purpose of a Corporation offer internal audit?

JOYCE You are referring to the Business Roundtable's

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

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

announcement in August 2019, when more than 180 CEOs committed to lead their companies for the benefit of all stakeholders. This represents a significant conceptual shift from their prior corporate governance statements, which have historically emphasized shareholder primacy as the dominant stakeholder. While it remains to be seen how effective this emphasis will eventually be, the idea that putting customers first, investing in employees and their local communities, engaging fairly and ethically with suppliers, and long-term value creation are directly connected to ultimately positive shareholder returns is certainly one that can be supported through internal audit assurance of the specific goals established to achieve measurable results.

YBARRA The potential here is huge, as it calls for the focus of the organization and its leaders to be broader than providing shareholder value. Auditors will need to consider how organizations generate value, in addition to their focus on revenue and expense drivers. For instance, concluding on the organization's ability to "support the communities in which we work" could be a monumental challenge for some internal auditors; however, focus on areas like this could help further differentiate and elevate an internal auditor's role and highlight those with dynamic abilities. It will be increasingly important for auditors to communicate with boards and leadership to ensure focus in assessing progress in these areas is supported and aligned with expectations.

What role should internal audit play in providing assurance over the information going to the board?

YBARRA The mission criticality and necessity of information going to the board should be assessed by internal audit and included, to some extent, in its engagement plan. Boards provide oversight and key approvals based on the information they are provided, and they must be assured that the information can be relied on. Deeper discussions with the executive team and audit committee regarding this level of assurance must occur to ensure their engagement and support.

JOYCE Clearly, recent survey results have demonstrated an inconsistent confidence level that boards receive the information they need to effectively manage strategic risks. To that end, chief audit executives (CAEs) might start by validating their audit committee's comfort with the level, depth, and timeliness of information they currently receive to satisfy their oversight responsibilities. Are the internal processes that compile this information designed to promote accuracy and transparency? What information provided is highly valued, and what information is ignored, or found not to be relevant? Obviously, time and effort should be devoted to facilitating those information streams that most directly relate to the board's strategic and governance accountabilities.

How can internal audit help address toxic cultures in an age when corporate behavior is under the microscope?

JOYCE There should be no tolerance in today's world for toxic corporate behavior. It drives away good employees, and will ultimately damage or destroy organizations that fail to identify and correct it. Internal audit is in an ideal position to continually assess the ethical and compliance environment within their organizations, and report opportunities for resolving gaps. They can partner with their compliance, legal, and human resource functions to ensure that employees are encouraged to report potential wrongdoing, and are supported and protected when they do so. They can ensure that any appropriate corrective or disciplinary action is applied timely, fairly, and consistently at all levels. They can measure the actions and examples set by senior management, and reinforce their critical responsibility to serve as behavioral role models. They can ensure that dialogue at the audit committee level includes frank discussions on these subjects when applicable.

YBARRA No. 1 is to take a position on identifying and rooting out issues with the culture. Auditors can get stymied by seeking undeniable criteria on which to base their conclusions. It will take: 1) creativity and communication to formulate and agree on the elements of culture that will be evaluated; 2) conducting engagements or including evaluation of these elements in every audit engagement; and 3) having the courage to report results, offer potential solutions, and follow up to ensure effectiveness and sustainability.

What skills should CAEs be looking for in new internal audit hires going forward?

YBARRA In evaluating potential hires, CAEs should be looking for an ability to listen, process, and demonstrate understanding before offering solutions. I've run across too many internal auditors who have answers before the problems are even identified. The mark—and genesis—of internal auditors is in their ability to listen. It's a basic skill that we need to continue to practice and teach.

JOYCE In many respects, the attributes of an effective new auditor haven't changed much in my 36 years in the profession. Basic technical skills will always be required, and the emphasis on adopting and maximizing emerging technology will continue to grow. Having a problem-solving and inquisitive nature also are important. However, soft skills are ultimately what sets a great auditor apart from an average one. The ability to effectively communicate, both verbally and in writing, is more difficult to teach a new auditor than how to sample accounts payable invoices, for example. Much of our job should be engaging with operational staff in a manner that makes them comfortable enough to share information and explain processes in a way that we may not have identified on our own. Ia

Aria

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

MARCH 16–18, 2020
General Audit Management Conference
ARIA Resort
Las Vegas

APRIL 5–7
Leadership Academy
Disney Yacht Club Resort
Orlando

JULY 19–22
International Conference
Miami Beach Convention Center
Miami

AUG. 17–19
Governance, Risk, & Control Conference
JW Marriott Austin
Austin, TX

SEPT. 14–15
Financial Services Exchange
Omni Shoreham
Washington, DC

SEPT. 16–17
Women in Internal Audit Leadership
Washington, DC

NOV. 2–4
All Star Conference
MGM Grand
Las Vegas

IIA TRAINING

www.theiia.org/training

JAN. 6–17, 2020
CIA Exam Preparation – Part 1: Essentials of Internal Auditing
Online

JAN. 14–23
Fundamentals of Risk-based Auditing
Online

JAN. 22–31
Building a Sustainable Quality Program
Online

FEB. 3–14
CIA Exam Preparation – Part 2: Practice of Internal Auditing
Online

FEB. 4–13
Root Cause Analysis for Internal Auditors
Online

FEB. 10–12
IT General Controls
Online

FEB. 11–14
Multiple Courses
Phoenix

FEB. 11–20
The Effective Auditor: Understanding and Using Emotional Intelligence
Online

FEB. 17–26
Fundamentals of IT Auditing
Online

FEB. 18–26
Multiple Courses
Lake Mary, FL

MARCH 2–5
Multiple Courses
Las Vegas

MARCH 2–11
Performing an Effective Quality Assessment
Online

MARCH 3–4
Data Analysis for Internal Auditors
Online

MARCH 10–19
Critical Thinking in the Audit Process
Online

MARCH 20
Fundamentals of Internal Auditing
Online

MARCH 30–APRIL 8
Enterprise Risk Management: A Driver for Organizational Change
Online

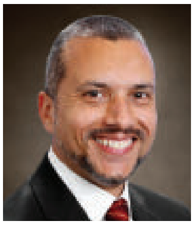
MARCH 30–APRIL 10
CIA Exam Preparation – Part 3: Business Knowledge for Internal Auditing
Online

MARCH 31–APRIL 9
Advanced Risk-based Auditing
Online

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

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

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



BY LUCIANO RAUS

CLIMATE RISK ASSURANCE

Financial institutions should consider the impact of climate change on daily operations and credit risk.

An article published earlier this year in *The Wall Street Journal* highlighted investor concern about the impacts of climate change, citing "a record of 75 or more climate-related shareholder proposals" expected at annual company meetings. Dupont investors, for example, proposed disclosure of the company's risks from expansion of its operations in hurricane-prone areas, and nearly 30% of Starbucks shareholders voted for disclosing the coffee giant's recycling plans. In addition, more and more institutional shareholders are backing the Sustainability Accounting Standards Board's standards for corporate sustainability, aimed at helping publicly listed companies disclose environmentally relevant information to investors. Internal auditors, and the organizations they serve, should take note of these developments—particularly in businesses where such concerns may not currently be a priority.

Within the financial industry, climate risk is not always on the agenda. For example, financial companies, and their internal audit functions, may neglect to consider the credit evaluation risks associated with lending money to companies susceptible to climate-related events. In doing so, lenders overlook impacts that could severely disrupt the borrowing companies' operations, and possibly hinder their repayment abilities. Even if it's discussed, resulting impacts to the company's credit risk rating may not be sufficiently accounted for when calculating the borrower's credit rating.

By contrast, insurance companies are at the forefront of addressing climate-related risk. Policy calculations, for example, factor in threats to homes and businesses in wildfire-prone areas and flood risk to regions susceptible to hurricanes. Financial institutions, however, typically do not include such considerations when calculating the impact of risk to capital. And even if bank leaders do incorporate climate-related impact in their credit risk analyses, there is no real metric in place for that risk.

As independent assessors of risk, internal auditors could raise the issue of climate change risk with senior management, and even consider it as a point of concern when challenging the organization's current risk management framework. Internal audit has the opportunity to create value, facilitate improvement, and execute its mission of providing independent assurance over the effectiveness of risk management. From envisioning the impact of climate-related risk on the bank's daily operations to the impacts on clients' operations and ability to perform against their credit risk, auditors can place themselves at the forefront of an important debate.

The financial industry, with the help of its internal audit practitioners, could get ahead of the curve by promoting a broad discussion about how to consider, monitor, and report climate change risk. If past crises taught us anything, reacting to stressed scenarios is arguably more expensive and takes longer to recover from than acting preventively. Let's start the debate—the sooner the better. Ia

LUCIANO RAUS, CIA, CFSA, *is a senior audit manager at Citigroup in New York.*

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