AUGUST 2019

A PUBLICATION OF THE IIA

Ia
INTERNAL AUDITOR

Machine Learning and Internal Audit

An Internet of Things Roundup

IIA Global Board Chair: Audit in Tune

Transforming Audit With Active Auditing

SECURING THE CLOUD

Complex cloud initiatives create a challenge for internal auditors.

CIA

Ia
INTERNAL AUDITOR

AUGUST 2019 VOLUME LXXVI: IV

FEATURES

Ia
INTERNAL AUDITOR

AUGUST 2019 VOLUME LXXVI: IV

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Intelligent Auditing Watch a data analytics expert discuss how internal auditors can use artificial intelligence to identify and assess emerging risks.

Relevance Amid Disruption To keep pace with today's constantly changing business environment, internal auditors must commit to continual learning and improvement.

The Ever-expanding Cloud A new report finds that most organizations doubt their security measures can keep up with the growth of the cloud.

The Benefits Swindler Employers, insurers, and regulators all have a stake in fighting workplace benefits fraud.

Find us on Facebook

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

COVER AND PREVIOUS PAGE: ILLUSTRATION BY DANIEL HERTZBERG; THIS PAGE,
TOP: DNY59 / ISTOCKPHOTO.COM, BOTTOM: WHO IS DANNY / SHUTTERSTOCK.COM

Editor's Note

FORTRESS IN THE CLOUD

Cloud computing has quickly risen to become a dominant business technology. Public cloud adoption, in fact, now stands at 91% among organizations, according to software company Flexera's State of the Cloud Survey. And it's only expected to grow from there. Analysts at Gartner say more than half of global enterprises already using the cloud will have gone all-in by 2021.

Collectively, that places a lot of responsibility for organizational data outside the enterprise. And while cloud migration can lead to significant efficiencies and cost savings, the potential risks of third-party data management cannot be ignored. Reuters, for example, recently reported that several large cloud providers were affected by a series of cyber intrusions suspected to originate in China. Victims, Reuters reports, include Computer Sciences Corp., Fujitsu, IBM, and Tata Consultancy Services. The news agency's chilling quote from Mike Rogers, former director of the U.S. National Security Agency, emphasizes the gravity of these breaches: "For those that thought the cloud was a panacea, I would say you haven't been paying attention."

As noted in this issue's cover story, "Security in the Cloud" (page 20), growing use of cloud services creates new challenges for internal auditors. Writer Arthur Piper, for example, points to issues arising from the cloud's unique infrastructure and the "lack of visibility of fourth- and fifth-level suppliers." He also cites the cloud's opaque nature and rapid pace of development as potential areas of difficulty. Addressing these issues, he says, requires internal audit to work with a wide range of business stakeholders—especially those in IT—and to secure staff with the right type of expertise.

The need to focus on these areas is supported by a recent report from the Internal Audit Foundation, Internal Auditors' Response to Disruptive Innovation. Among practitioners surveyed for the research, a consistent theme emerged with regard to cloud computing—to be successful, internal audit should build relationships with IT, before moving to the cloud. Multiple respondents also recommend bringing in personnel with specialized IT skills to facilitate the evaluation of cloud controls. Moreover, they noted the importance of evaluating not only standard internal controls in areas like data security and privacy, but soft controls, such as institutional knowledge, as well.

Of course, cloud computing is only the tip of the iceberg when it comes to challenges around disruptive technology. Among other IT innovations affecting practitioners, artificial intelligence and the Internet of Things are equally impactful. We examine each of these areas in "Stronger Assurance Through Machine Learning" (page 27) and "Wrangling the Internet of Things" (page 32), respectively. And be sure to visit the Technology section of our website, InternalAuditor.org, for insights and perspectives on other IT-related developments affecting the profession.

David Salierno

Reader Forum

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

Ia
INTERNAL AUDITOR
A Risk Management Case Study
North American Board Chair: It's Time to Step Forward
Thwarting Bias in AI
The Audit Committee Ethics Expert
THE CLEAR CHOICE
Mounting evidence shows better business performance for organizations that choose an ethical path

Social Media Risk

The article on auditing social media is well-timed. Recent issues that many organizations and individuals have faced with social media call attention to another area where internal audit can provide value-added services. Internal audit could use Milosavljevic's article as a framework to develop audit programs that help organizations and individuals minimize reputational and financial risks to their brand and bottom line.

FREDRICK LEE *comments on Maja Milosavljevic's "How to Audit Social Media" ("Risk Watch," June 2019).*

Milosavljevic raised good points to help organize and structure the topic. One (very) gray area that remains elusive is the extent to which an organization should dictate the behavior of its employees on their own personal pages. Guidelines should naturally be provided in terms of how to (or not to) refer to the company or situations or opinions involving the company, but enforcement would be very limited. This is probably a topic to be included in the Code of Ethics, but legal should always be consulted to establish the appropriate boundaries, so I'd add that to procedures that should be verified by internal audit.

BRENO GALVAO *comments on Maja Milosavljevic's "How to Audit Social Media" ("Risk Watch," June 2019).*

Auditing Culture

I think Jim Roth made some good points: Engage others and consider the current culture. I also would include: 1) compliance, risk, and human resources as key stakeholders; and 2) understand current culture/employee surveys, not just a selected model. Also, we need to get back to basics in terms of IIA standards and better understand what culture is and how much we can realistically assure it.

J. PATERSON *comments on Jim Roth's online series "Auditing Culture: Where to Begin?" (InternalAuditor.org).*

Auditor as Consultant

Providing advice and sharing information with management could help promote the image of the internal audit function within an organization. However, auditors must be comfortable doing so, as there is no such "reviewer" to oversee the discussions or, depending on the type of consulting activities, the report. If an auditor feels uncomfortable doing so, he or she could speak directly to the head of internal audit to express clearly why he or she feels uncomfortable providing consulting services or participating in the consulting activity. After all, not everyone is trained to be a consultant.

LAURENCE LAU *comments on the Points of View by Pelletier blog post, "Independence: A Tool, Not a Shield" (InternalAuditor.org).*

Ia
INTERNAL AUDITOR
AUGUST 2019
VOLUME LXXVI:IV

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design

PRODUCTION MANAGER
Gretchen Gorfine

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

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

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

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

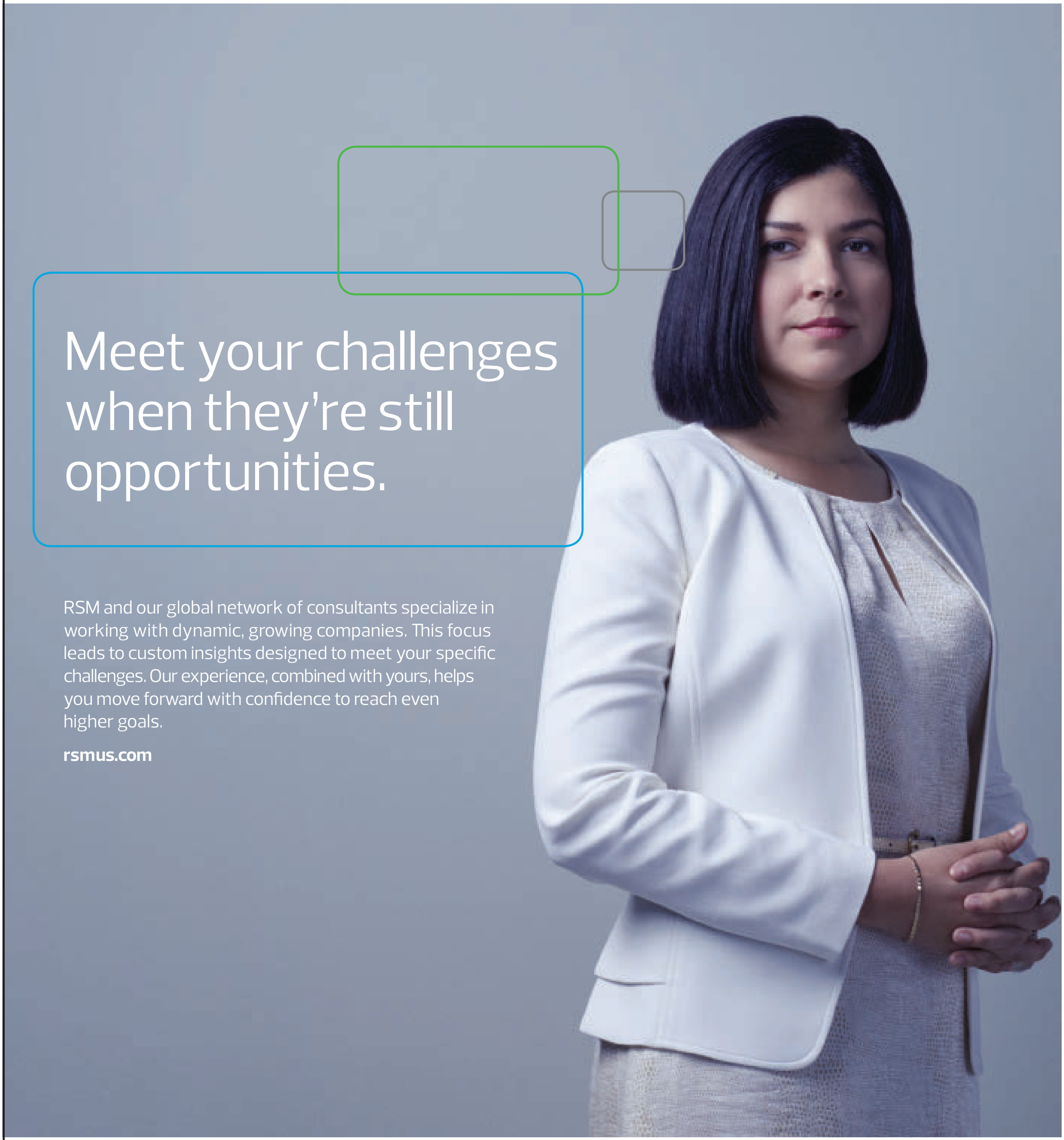
ADVERTISING
sales@theiia.org
+1-407-937-1388; fax +1-407-937-1101

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")



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

rsmus.com

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

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

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

Boards seek disruption guidance... Consumers worry about personal data... Firms respond to shifting tariffs... Companies foresee costly climate risks.

Update

INDUSTRIAL THREATS LOOM LARGE

Security practitioners worldwide say cyberattacks significantly threaten industrial control systems (ICS).

50% rank ICS security threats high or severe/critical.

62% identify people as the greatest risk for compromise.

24% worry about phishing, despite its frequent use in ICS attacks.

Source: SANS Institute and Nozomi Networks, SANS 2019 State of OT/ICS Cybersecurity Report

ETHICAL EXPECTATIONS

Ethics and compliance programs need to focus on changing behavior.

Despite more organizations embedding ethics and compliance (E&C) programs into operations, employees say they feel discouraged from reporting ethics violations, and most aren't comfortable talking about ethical issues in meetings.

According to New York-based LRN Corp.'s 2019 Ethics and Compliance Program Effectiveness Report, organizations struggle to implement E&C programs that work well in practice, often still focusing more on rules and prohibitions and too little on shaping employee behavior. "Employees need a good moral compass," says Susan Divers, an advisor at LRN. "They don't need a five-pound manual as a guide."

Most of the 480 E&C professionals surveyed globally say the number of board members who are actively invested in promoting ethical behavior in their organizations is low. Moreover, just 49% say management at their organization acts against compliance failures, 38% say leaders discipline high performers who are guilty of misconduct, and 22% say their organization communicates lessons learned and remediation measures taken after an ethical lapse.

On a positive note, 87% of respondents say their organization's E&C program increasingly focuses on values over rules, up from 44% in 2018. Additionally, more than

IMAGES: TOP, DNY59 / ISTOCKPHOTO.COM; LEFT, FIDART / SHUTTERSTOCK.COM

FOR THE LATEST AUDIT-RELATED HEADLINES follow us on Twitter @TheIIA half say ethical behavior is now a major factor in their organization's employee performance reviews, up from 35% in 2018.

Organizations that include E&C in every phase of decision-making not only outperform the competition, they enable their employees to act based on shared values rather than minimum legal requirements and short-term expediency, the report notes. Those E&C programs that play a broad role as corporate conscience are four times more likely to have a positive impact on employees' levels of speaking out. **— S. STEFFEE**

NOT READY FOR DISRUPTION

Boards should seek guidance on overseeing digital changes.

Nearly half of corporate directors say their board lacks the resources needed to guide their companies through technological disruption, a *Corporate Board Member* magazine and Ernst & Young LLP study reports. Indeed, directors say they have greater confidence in management's ability to address disruptive change than they have in the board's acumen.

Indeed, most boards rely primarily on management briefings to stay abreast of industry trends and technology innovations, according to the How Boards Are Governing Disruptive Technology report. These developments aren't showing up regularly on the board's agenda, though. Only three in 10 boards discuss emerging technologies regularly, while nearly half discuss them on an ad-hoc basis.

"Directors should embrace a learning mindset," says Steve Klemash, Americas leader for EY's Center for Board Matters. In addition to management, Klemash recommends directors seek advice from external experts to increase the board's technology competency.

To get boards started, the report suggests directors look at whether they are allocating sufficient time to oversight of innovation and disruption, and whether the board has relevant expertise. They also should leverage external data on disruptive risks and identify innovation-related metrics. **— T. MCCOLLUM**

34%

OF CYBERSECURITY LEADERS

have high confidence in their cybersecurity team's ability to address cyberthreats.

43%

SAY THEIR TEAM REPORTS

to a chief information security officer, and 27% report to a chief information officer.

"When the cybersecurity team reports directly to a designated and experienced cybersecurity executive, cybersecurity teams report having significantly more confidence in their team's capability to detect attacks and respond effectively," says Frank Downs, director of ISACA's cybersecurity practices.

Source: ISACA, 2019 State of Cybersecurity Study

CONSUMERS WARY OF DATA COLLECTION

Two surveys point to apprehension over sharing personal data online.

Security concerns are impacting the way consumers interact with organizations online, according to new research. In the U.K., a survey of more than 2,000 adults by London-based digital services provider Studio Graphene found that 16% suffered an online banking, social media, shopping, or email account hack within the last year. Subsequently, nearly one-fifth say they stopped using social media, 12% changed service providers (including banks, utilities, and streaming services), and 6% switched to a different email provider.

Moreover, nearly three-fourths of respondents say they are now mindful of

IMAGES: TOP, RAWPIXEL / ISTOCK.COM; RIGHT, BSWEI / SHUTTERSTOCK.COM

CALIFORNIA 2019

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

PLATINUM

protiviti®
Face the Future with Confidence

RSM

SILVER

EY
Building a better
working world

Grant Thornton

BRONZE

BLACKLINE

Crowe

onapsis

OneTrust
Privacy Management Software

pwc

Tempus Resource
by ProSymmetry

IIA®
The Institute of
Internal Auditors
Southern California Chapters

IIA®

MORE VISIT InternalAuditor.org to read an extended interview with Matthew Bonavita.

which mobile apps and websites they supply personal information to. Another 70% are cautious of the networks and devices they use to share sensitive information.

A separate survey shows similar concerns in the U.S. Nearly two-thirds of U.S. consumers "are seriously concerned … about the unauthorized access to or misuse of their personal information," according to Unisys, an IT services company in Blue Bell, Pa. In addition, more than half are seriously concerned about their credit card data being stolen.

The survey's authors say the results of the 2019 Unisys Security Index speak to a widespread perception that consumers do not trust companies that keep their personal data. "Businesses and government agencies that hold this type of data on their clients or constituents should make its protection the highest priority, while clearly communicating the steps they are taking to keep it safe," the report says.

The Unisys study recommends several such steps businesses and governments can take to address consumer concerns. Suggestions include moving toward a security model that assumes all network traffic is a potential threat and addressing risks pertaining to the proliferation of devices in and around the workplace. The report also recommends using biometrics and other technology to help verify customer identity. **— D. SALIERNO**

THE WINDS OF TRADE WARS

Compliance with changing U.S. tariff policies requires a robust response plan, says Matthew Bonavita, director of internal audit at New Balance.

How can a global company determine how to comply with volatile trade regulation shifts? In a changing global landscape, organizations need to be aligned, agile, and prepared. Specific to tariffs, the compliance office, supply chain, and public affairs/regulatory teams need to work together to develop a comprehensive response plan. In an escalating trade war, all functions need to understand their roles within the plan and be agile enough to ensure timely implementation. Items to prioritize are reviewing third-party contracts, updating costing models, investigating alternative supply options and coordinating with logistics, and ensuring controlled processes are in place to comply with changing duty rates and classifications.

As a risk leader within the organization, internal audit first should vocalize and elevate the potential impact of geopolitical risks, including trade wars and tariffs, to the audit committee, senior leadership, and others within the business. Second, internal audit should work with the appropriate teams to ensure response plans are in place if trade wars escalate or continue for an extended period. Third, internal audit should review the customs compliance process, paying particular attention to classification procedures and documentation to minimize the risk of transshipment [through intermediate sites] and payment noncompliance.

COUNTING CLIMATE'S COSTS

Companies have much to risk and gain from climate change.

Climate change risks could cost the world's biggest companies $1 trillion, London-based environmental disclosure firm CDP reports. Many of these risks could happen within the next five years, the study of 215 global companies notes.

And just 15% of the 500 largest global companies are in line with the Paris climate accord's goal of limiting global warming to below 2 degrees Celsius by 2100. That's according to a separate *Financial Times* analysis of data compiled by Zurich-based climate analysis group Carbon Delta AG.

"The goalposts for climate action have never been clearer for companies," says Nicolette Bartlett, CDP's director of climate change. CDP reports that eight in 10 companies say they expect major climate impacts on their business, with companies rating climate costs as likely to virtually certain to reach $500 billion.

There is a silver lining, though. Companies tell CDP that climate change could create $2.1 trillion in new business opportunities such as increased demand for low emissions products and services. **— T. MCCOLLUM**

PHOTO: RIGHT, IMAGEDEPOTPRO / I-STOCK.COM

BY ALEX RUSATE EDITED BY JAMES ROTH + WADE CASSELS

EXPAND YOUR ROLE IN INTERNAL AUDIT

Keeping up to date and seizing opportunities can help novice auditors advance in the profession.

How does a new internal auditor whose primary focus could be standard audits, such as auditing expense reports or U.S. Sarbanes-Oxley Act of 2002 testing, get the opportunity to work toward auditing nontraditional risks that are strategically significant to the company? Internal audit departments cannot audit what matters if it keeps new auditors on an island regarding internal and external information and changes facing their companies. By capitalizing on information and best practices, internal auditors can expand their roles both within the department and the organization. This is especially beneficial with the changing demands of stakeholders, senior management, and regulators.

Internal Information

Through a blend of formal and informal channels, internal auditors can keep their fingers on the pulse of the company and identify opportunities to add value. There are many formal conduits of information that can yield useful information about potential audit opportunities. Having internal audit participate in financial close calls and quarterly business reviews is a great way to identify the company's pain points and potential solutions.

For example, suppose while sitting in on a call, management notes that due to recent turnover and capacity issues, accounting was unable to identify the root cause of an issue related to absorption accounting at one of the production plants. The chief audit executive (CAE) volunteers one of his or her auditors to assist at an advisory level to do a root cause analysis and help develop an operational process narrative to help new employees understand the process. The auditor identifies issues that were causing absorption to be underreported at the plant, which, in turn, increased expenses. By remedying these issues, the plant is able to accurately present its financials and drive higher profitability.

Informal Communication

Internal auditors can get exposure to critical information through the simplest means. Developing professional relationships with different departments opens the door to many audit opportunities. It could be as easy as informally discussing issues facing their department that could expose process flaws or opportunities for improvement. This can be done by encouraging the audit team to sit with different departments in the company cafeteria instead of isolating themselves by sitting with other auditors.

Informally engaging with other departments also may turn up issues that

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

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

aren't discussed in formal meetings. For example, suppose an auditor invites her company's operations manager to lunch. While trading pleasantries, the manager mentions that an employee quit his job a week before and left his badge and corporate credit card on his desk. No one has come to retrieve it and the items have been sitting out in the open ever since. The auditor is concerned, so she tests the badge at the entrance and it still unlocks the door. With her CAE's approval, the auditor reviews the exit process and discovers that 80% of employees who left or were fired that year still had access to the building, and that there was no formal offboarding process to ensure that badges were collected. The issue is then quickly remedied, but it may have persisted if the auditor had not decided to lunch with the operations manager.

External Information

Subscribing to industry publications and tracking standards and regulatory updates can help internal auditors gain a better understanding of the company, itself, and the industry their company is in. Greater knowledge of these areas improves an auditor's capability to indentify risks.

> Staying current on relevant standards allows internal auditors to identify issues and address them proactively.

Industry Publications Knowing how the industry is operating and trending can help identify risks, drive efficiencies, and create competitive advantages. Internal auditors can subscribe to industry publications or create Google alerts for their companies and competitors to easily stay informed about industry news and make educated assessments of risk.

Standards Updates Staying current on relevant standards updates before their adoption dates allows internal auditors to identify issues their company might face and help address them proactively. When a new standard is adopted, instead of waiting for the evaluation and adoption to be completed by management, internal auditors can study the topic and develop the required competencies. Then they can discuss with their CAE their interest in joining the implementation team as an advisor.

At this level, auditors can be proactive in providing insight into the adoption controls that should be in place throughout the project and the process-level controls that should be embedded into the procedures during implementation. Major public accounting firms often release resources such as industry-specific interpretations and practical applications of standards updates for free.

Regulatory Updates It is important to keep track of regulatory changes for smaller companies that don't have the resources to proactively disseminate regulatory information to their employees. For example, if an employee was not aware of a regulation such as the U.S. Telephone Consumer Protection Act (TCPA), which prohibits solicitation to phone numbers that are listed on do-not-call lists and the company uses robocalling for commercial solicitation, they could be exposing the company to risk. Or if it relied on data obtained by a third party saying it supposedly was already scrubbed against all numbers on state and national do not call registries, then making calls from that list could open the company up to class-action lawsuits if those numbers were opted in to a do-not-call registry. Since the TCPA is a strict liability statute that awards $500 per violation and up to $1,500 per willful violation, a class-action lawsuit with thousands of violations could have a material impact on the company.

Internal auditors can be a great resource by identifying regulatory risks such as these based on their knowledge of processes and staying current on regulatory laws and updates. This is a great example of how an auditor can step outside of his or her comfort zone to audit what matters to management. One caution when stepping out of comfort zones is to remember IIA Standard 1210: Proficiency. If an auditor does not have the competency to conduct the audit or review, he or she should not begin it.

Grow Your Career

Through leveraging internal and external information and capitalizing on change, internal auditors can position themselves to expand their roles and develop skills that will help them advance their careers. This includes staying informed and keeping their eyes open, continuing professional development, staying involved, inviting themselves to formal and informal corporate meetings, and ensuring they are prepared to deliver on engagements. Ia

ALEX RUSATE, CIA, CRMA, CCSA, CPA, *is senior associate, risk consulting in IT Audit and Assurance, at KPMG in Albany, N.Y.*

BY JAMES BONE EDITED BY STEVE MAR

TRANSFORMING ASSURANCE

Data analytics and automation can enable internal audit to provide enhanced assurance for organizational risks.

The IIA's Core Principles for the Professional Practice of Internal Auditing use the term *risk-based assurance* instead of *reasonable assurance*, which implies that there are different levels of assurance based on multiple risk factors. That creates an opportunity for internal audit to move its work to a higher level by delivering *enhanced* assurance to the board and management.

Enhanced assurance does not imply reductions in risk. Instead, it refers to asking better questions about the risks that matter as well as the risks that should be automated for greater efficiency. It's about developing assurance at scale to cover the breadth of operations and strategic initiatives efficiently and cost-effectively.

Computerized fraud detection is one example of delivering assurance at scale. In 2002, WorldCom internal auditor Gene Morse discovered a $500 million debit in a property, plant, and equipment account by searching a custom data warehouse he had developed. Morse's mining of the company's financial reporting system ultimately uncovered a $1.7 billion capitalized line cost entry made in 2001, according to the *Journal of Accountancy*.

This example illustrates how fraud or intentional errors can occur in limited transactions with catastrophic outcomes. Enhanced assurance techniques such as data mining can uncover these transactions, which traditional audit techniques such as discovery, stratification, and random sampling may miss. Today's technologies can enable internal audit functions to automate their operations and provide enhanced assurance, but to do so, they must reframe their strategy.

Better Teams

Data analytics and audit automation platforms provide internal auditors with the means to build assurance at scale whether a novice or expert. The technologies also create the opportunity to form better teams.

Small, focused teams are more productive than large, consensus-driven teams directed from the top down, author Jacob Morgan notes. Writing in *Forbes*, Morgan cites Amazon CEO Jeff Bezos' "two-pizza" rule: "If a team cannot be fed by two pizzas, then that team is too large." Morgan says having more people on the team increases the communication needed and bureaucracy, which can slow the team down.

Collaboration with automation can modernize the performance of small teams. Intelligent automation can integrate oversight into operations, reduce human error, improve internal controls, and create situational awareness where risks need to be managed. Automation-enabled collaboration can help reduce

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

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

redundancies in demands on IT departments, as well. However, efficiency transformations often fail when projects underestimate the impact of change on people.

The Human Element

Many of the biggest assurance risks are related to people, but too often the weakest link is related to auditing human behavior. The 2018 IBM X-Force Threat Intelligence Index finds "a historic 424% jump in breaches related to misconfigured cloud infrastructure, largely due to human error." IBM's report assumes decisions, big or small, contribute to risks. However, the vulnerabilities in human behavior and the intersection of technology represent a growing body of risks to be addressed.

Separate studies from IBM, the International Risk Management Institute, and the U.S. Department of Defense find that human error is a key contributor to operational risk across industry type and represents friction in organizational performance. The good news is automation creates an opportunity to reduce human error and to improve insights into operational performance. Chief audit executives (CAEs) can collaborate with the compliance, finance, operations, and risk management functions to develop automation that supports each of these key assurance providers and stakeholders.

The Role of Technology

Technology enables enhanced assurance by leveraging analytics to ask and answer complex questions about risk. Analytics is the key to finding new insights hidden within troves of unexplored data in enterprise resource planning systems, confidential databases, and operations.

Technology solutions that improve situational awareness in audit assurance are ideally the end goal. Situational awareness in auditing is not a one-size-fits-all approach. In some organizations, situational awareness involves improved data analysis; in others, it may include a range of continuous monitoring and reporting in near real-time.

Intelligent automation addresses issues with audit efficiency and quality. First, auditors spend, on average, half their time on routine processes that could be automated, improving consistency of data and reductions in error rates. Data governance allows other oversight groups to leverage internal audit's work, reducing redundancy of effort.

Second, smart automation leads to business intelligence. As more key processes are automated, they provide insights into changing conditions that may have been overlooked using periodic sampling techniques at points in time.

Most events are high frequency but low impact, yet auditors, IT staff, and risk and compliance professionals spend the bulk of their time chasing down these events. That leaves little time for them to focus on the real threats to the organization. Automation works best at solving high frequency events that are routine and add little value in terms of new information on known risks. Instead of focusing on the shape of risk, auditors will be able to drill down into the data to understand specific causes of risk.

Steps to Enhanced Assurance

Before buying automation, CAEs should answer three questions: How will automation improve audit assurance? How will automation make processes more efficient? How will auditors use it to improve audit judgment?

The CAE should consider automation an opportunity to raise awareness with the board and senior executives about enhanced assurance and better risk governance. To do so, internal audit must align enhanced assurance with the strategic objectives of senior executives.

To implement enhanced assurance in the internal audit function, CAEs should follow three steps:

- Identify the greatest opportunities to automate routine audit processes.
- Prioritize automation projects during each budget cycle in coordination with the operations, risk management, IT, and compliance functions.
- Consider the questions most important to senior executives: Which risks pose the greatest threat to the organization's goals? How well do we understand risk uncertainties across the organization? Do existing controls address the risks that really matter?

Assurance and Transformation

The World Economic Forum calls today's digital transformation the fourth Industrial Revolution and forecasts that it could generate $100 trillion for business and society by 2025. Every business revolution has been disruptive, and this one will be no exception. The difference in outcomes will depend largely on how well organizations respond to change.

Forward-looking internal audit departments already are delivering enhanced assurance by strategically focusing on the roles people, technology, and automation play in creating higher confidence in assurance. Other audit functions are in the early stage of transformation. Although these audit functions will make mistakes along the way, now is the time for them to build new data analysis and data mining skills, and to learn the strengths and weaknesses of automation. As these tools become more powerful and easy to use, enhanced assurance will set a new high bar in risk governance. Ia

JAMES BONE *is lecturer in discipline enterprise risk management at Columbia University in New York and president of Global Compliance Associates in Lincoln, R.I.*

Fraud Findings

BY SCOTT MARK EDITED BY BRYANT RICHARDS

GUILT BY ASSOCIATION

A membership organization pays a hefty price after handing over too much control to its management company.

Olivia Munro, a hospital chief financial officer (CFO) and former pharmacist, was approached about the treasurer position with her state's pharmacy organization, which was experiencing sustainability issues. The organization's finances and membership numbers were in decline, and the board was struggling to lead through these challenging times. Out of a sense of professional obligation, she agreed to serve in the role. Never having served on a professional board, Munro did not know what to expect.

The small association of approximately 750 members charged an annual fee of $350, which included educational programming to satisfy mandatory continuing education requirements for professional licensure. Most of the revenues, however, came from an annual educational meeting that charged a registration fee to attend. The meeting was poorly attended, so most revenue came from pharmaceutical manufacturer grants for advertising.

After joining the board, Munro quickly realized that the organization had exhausted the available and willing volunteers within the state. Subsequently, it recruited fewer qualified people into leadership roles and recycled previous leaders. With the focus of the organizational leadership on the professional mandate, the financial affairs had been placed in the hands of underqualified individuals with limited fiscal acumen. As a result, this once-healthy organization became insolvent and contracted with an external professional management company specializing in turning around professional organizations.

Historically, the organization had several decades of financial success, accumulating $500,000 in reserves for operating purposes and an additional $250,000 in restricted funds to support scholarships for students in underserved communities. Although the organization previously had a treasurer, his limited financial expertise was evident in the lack of financial controls in place.

Munro wanted to determine the status of the organizational books that she was inheriting, so she conducted a review of them to make sure transactions had supporting paperwork, there were not any unusual transactions, and that the bank balances reconciled. She had several questions regarding the language in the contract with the management company and learned that it was signed without legal review. In particular, the contract contained a confusing evergreen clause perpetuating the relationship on a mandatory three-year cycle, rather than typical one-year extensions. Further, the contract did not contain a termination clause. The fee structure was equally complicated, with various

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

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

LESSONS LEARNED

- » Outsourcing relationships and contracts should be reviewed by internal audit for control weaknesses before implementation and before any significant changes. There is an opportunity for internal audit associations to share guidelines with nonaccounting associations to improve financial practices and protections.
- » Internal audit should ensure management has processes in place to monitor contract requirements on a regular basis. The absence of these reviews leads to undetected issues and the inability to optimize the value of the relationship.
- » Organizations that don't segregate financial duties open themselves up to misappropriation of funds and fraud.
- » Failure to maintain signatory authority can prevent organizations from legally accessing their own banking information for audit.
- » Regardless of the professional nature of an organization, knowledgeable financial people should be assigned to monitor its finances.
- » If the outsourced relationship fails to produce financial statements and banking documents regularly, it should prompt an immediate review and rigorous follow-up.

a la carte upcharges that were poorly defined. This made it difficult to clarify which services were included in the initial contract and what was added on.

The relationship had been positive and the organization eventually transitioned additional authority to the management company, which was not reflected in a contractual amendment and instead was governed by email communications. This included managing the organization's website and membership database and organizing the annual meeting. As part of this transition, the organization's official mailing address was also changed to that of the management company, and the company was given signatory authority on the organization's bank accounts. It appeared that the management company had complete control of the organizational finances and operations.

Over time, the management company's level of service began to decline. The assigned management representative failed to attend board conference calls and provide contractual information such as monthly financial reports. In addition, bank statements were no longer being provided for review and reconciliation by the treasurer, and requests for status updates were responded to with increasingly vague answers.

Munro feared that the organization's funds had been fraudulently misappropriated and requested access to the organizational paperwork. Requests were repeatedly ignored or incompletely fulfilled. The management company was located in an adjacent state, so a local accountant was hired and law enforcement was notified to gain access to the records. Records were limited and those that were available had sloppy documentation, making it impossible to track payments and expenses accurately. Bank statements showed that $300,000 of the organization's funds were spent and current hotel expenses of $120,000 from the annual meeting had not been paid.

The organization obtained legal counsel and additional discovery followed. During the previous year, the management company had systematically billed the organization $100,000 for a la carte fees associated with ill-defined activities not specifically outlined in the contract. Because the management company was given authority to pay itself directly from the organization's bank account, and had used the a la carte provisions to generate repeat charges not reviewed by organizational leadership, legal counsel did not think it would be possible to recover these damages. The fact that the organization had not received the monthly bank statements to question these practices was considered gross negligence on behalf of the organization.

The remaining $250,000 from the restricted funds was also missing. When challenged, the management company refused to supply it, citing that the original contract had auto-renewed for an additional three-year period under the evergreen clause. The organization had failed to exercise the contractual 90-day notice period and, as a result, the remaining funds were due to the management company to satisfy the three-year extension on the contract. The organization's board concluded, with input from legal counsel, that the legal fees would be more than the organization could potentially gain. The management company filed for bankruptcy and subsequently reopened under a new name.

The management company had control of the organization's website, domain name, and membership lists, and ultimately, it agreed to return control to these proprietary operational elements and both sides walked away. The organization began to rebuild, and Munro set up appropriately designed financial controls. Shockingly, the membership reelected the same board, and Munro made the decision to step down from her role as treasurer. ia

SCOTT MARK, PHARMD, *is vice president at Craneware Healthcare Intelligence in Pittsburgh.*

Security in the Cloud

The growing use and increased complexity of cloud computing is creating new challenges for internal auditors.

Arthur Piper

Illustration by Daniel Hertzberg

Although Jean-Michel Garcia-Alvarez was used to working as a high-level internal auditor in the financial services sector, 2015 presented him several novel challenges. First, he was appointed head of internal audit—and later also data protection officer—at a new, fintech challenger bank in London called OakNorth. It had received regulatory approval from both the Prudential Regulatory Authority and the Financial Conduct Authority in August 2015—one of only three U.K. banks to do so in the past 150 years. Second, OakNorth wanted to be the first U.K. bank with a cloud-only IT infrastructure, which was not an area he specialized in during his previous audit roles at Nationwide Building Society, RBS, or Barclays.

Garcia-Alvarez realized that traditional audit skills would be of limited use because of the cloud's newness and evolving nature, with little precedent in the scope and range of how to approach it as an internal auditor. So, he decided to obtain an IT audit certificate from the U.K.'s Chartered Institute of Internal Auditors (CIIA). It boosted his IT audit skills and forced him to get to grips with how to approach cloud auditing and security. It also made him a credible security player in the business.

At the same time, he says internal auditors must adhere to the fundamental remit of audit, which, for OakNorth, is the CIIA's Financial Services Code. One of the first sentences of that document says internal audit's primary role is to help

senior management protect the assets of the business—in this case from hacking, data breach, and leakage.

"That is absolutely the role of internal audit in cloud security," Garcia-Alvarez says. When businesses are migrating to and operating in the cloud, internal audit needs to provide assurance that the cloud infrastructure is safe, secure, and able to meet the firm's objectives—not just now, but in the future. "The way to do that is to be embedded as the third line of defense and to provide real-time feedback on risk and controls, and to assure the board that you are mitigating risk with data—not creating new ones."

While cybersecurity has long been on auditors' lists of regular assignments, securing today's cloud poses fresh challenges. The very structure, speed, and opacity of the cloud demands a focus away from traditional auditing. Having systems in place to deal with data breaches, data loss, and ransomware attacks is mostly standard today, but dealing with the security issues arising from the unique infrastructure of the cloud, the lack of visibility of fourth- and fifth-level suppliers, and the need to work in tandem with both the cloud provider's own security teams and a wider range of stakeholders across the business are growing challenges for internal auditors dealing with cloud security.

"The biggest problem in these virtual environments is that the distance between control and assurance gets wider."

James Bone

"The way to [provide assurance] is to be embedded as the third line of defense and to provide real-time feedback on risk and controls."

Jean-Michel Garcia-Alvarez

CHANGING PURPOSE

OakNorth's journey is a good example of how the speed of change impacts internal audit's security concerns. Like many businesses, OakNorth's cloud provider in 2016 was Amazon Web Services (AWS). As a large global player, Garcia-Alvarez was happy that AWS could be responsible for the security of the cloud, while OakNorth was responsible for security in the cloud. That theoretically makes it easier for internal audit because the function can regularly check and rely on the up-to-date certifications maintained by the cloud provider. Audit can then focus almost entirely on the internal security control environment. In reality, though, for cloud security to be robust auditors also need to keep up with changing laws, rules, and regulator expectations.

"Those can change very quickly," he says. In 2016 when OakNorth migrated to the cloud, the U.K. financial regulator was happy with the decision and with the company's cloud provider—because it was big, safe, and secure. But when other banks followed suit by 2017, the regulator decided it was a potential concentration risk. If AWS went down, it would take a huge slice of the U.K. financial services sector with it. As a result, OakNorth moved to a multi-cloud solution for all of its client-facing technology.

From the outset, OakNorth used cloud data centers, provided by AWS, in several locations in Ireland, with an additional fail-safe elsewhere in Europe. "That one is like a bouncy castle," Garcia-Alvarez says. "The shell is there, but the engine is off. Turn on the engine and it will be fully blown up and working in a matter of hours." Just to be sure, the IT team rebuilds the core banking platform from scratch at a new location in Europe once a year, with internal audit providing independent assurance over the exercises. "It is time-consuming and expensive, but at least we know that the bank is safe."

GETTING IN EARLY

Cloud downtime is not a fantasy risk. In February 2017, for instance, AWS services on the U.S. East Coast experienced failure. While reports on technology news site *The Register* suggested the servers were down only about half an hour, some customers reportedly could not get their data back because of hardware failure. Another outage in March 2018

More than 50% of businesses say they operate within a complex cloud environment, including multiple clouds and hybrid clouds, according to a 2019 Cloud Security Alliance survey.

affected companies such as GitHub, MongoDB, NewVoiceMedia, Slack, and Zillow, according to CNBC.

James Bone, a lecturer at Columbia University and president of Global Compliance Associates in Lincoln, R.I., says that is just one of many reasons internal auditors should be involved early in any cloud deployment. "I don't believe that internal auditors should be deciding which products to use, but I do think they should be very much involved in the selection process," he says. "They need to understand the service model, what is being deployed, and how they are planning to use the services. The platform that they use will determine, to a large part, the risk exposure to the firm."

That is because the choice of platform governs what data will be transitioned, if any will stay on the premises, access administration, business continuity plans, data breach response, ransomware strategy and response, the frameworks the service provider uses for cloud security, the frequency of monitoring, contractual agreements, and many other factors. Auditors need to be on top of the situation to raise red flags before security risks crystallize. Bone says, for instance, that he has heard stories of service providers failing during a transition to the cloud, without a backup in place from which to restore the client's data. In this example, organizations need to know what the recovery plan is and, crucially, who is responsible for it.

SHARING RESPONSIBILITY

"These are shared security and operational relationships between the cloud provider and the business," Bone says. "So it is about clearly separating the different lines of accountability and responsibility at an early stage." That includes sharing operational performance metrics and having clear escalation processes for data breaches, outages, and other security issues where the responsibilities are set out clearly between the cloud provider and the business. The internal audit team must have a realistic understanding of its own and the business's capabilities if those measures are to be effective. "If the firm and the audit team are not particularly agile, can they use the vendor to take up some of that role?" he asks.

The opaque nature of what goes on in the cloud service provider's business is a particular worry for internal auditors. "The biggest problem in these virtual environments is that the distance between control and assurance gets wider," he says. Bone has been researching this idea for about four years. In digital environments, he says, risk and audit professionals have been used to testing applications because in most cases the physical hardware and data are available to see, touch, and analyze.

"As we move to a boundaryless environment, we are creating a distance between our ability to recognize a problem and having to rely on others to tell us there is a problem," he says. "That distance impacts response time, and our ability to develop and put in place even more robust controls, because we are further away from the problem. This is an underappreciated risk and is getting larger because firms that are providing these services are getting better at managing their own risk, while as businesses go further into the cloud and have multiple cloud providers, they are becoming more removed from core processes."

Auditors must stay informed and raise red flags before security risks crystallize.

POTENTIAL HEADACHES

For Fred Brown, head of the critical asset management protection program at HP in Houston and former head of IT audit at the firm, dealing with cloud security while working with such shared services can create "rather large challenges."

"The more you open your environment, the more you have to stay on top of security," he says. Over the last couple of years, HP has been working toward being a top quartile security organization, he explains. And Brown's cyber team has grown 70% during that time. The business has been aggressively moving to cloud services — including infrastructure as a service, platform as a service, and software as a service. Implementing a 100% review of all suppliers that would include all cloud instances throughout the business means doing a detailed security check of more than 2,000 suppliers across the enterprise.

To speed up the process, HP has contracted with a third-party assessment exchange, Cyber GRX, which describes itself as supplying "risk-assessment-as-a-service." Any subscriber can have a supplier risk assessed — once the results are in, users can view them via an exchange. The process is integrated into HP's inherent risk-scoring program, so that all vendors except those with the highest inherent risk score are assessed by Cyber GRX. The vendors with the highest inherent risk are risk assessed by internal resources. This process represents a new initiative at HP, and so far it has produced useful reports

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

> "Every time you make a change to the group policy, it cascades to all the instances that are underneath that."
>
> Fred Brown

and helped the company tackle a backlog of risk assessments.

"This is removing an entire blind spot when it comes to risk," Brown says. "Even if you have 100 suppliers who you haven't assessed, with many connected to your company's critical assets, whether it is employee data, or something else—if you haven't assessed them, you have no idea what their risk profile really looks like."

Brown says one problem is that whether a cloud-based supplier is AWS or a small online education provider, if it is managing critical data, the threat to the business is the same. With many cloud providers now outsourcing parts of their own operations, HP is putting in extra effort on fourth- and fifth-party risk management. That is why having someone track the cloud supplier landscape is critical to managing security risk, he says, enabling the organization to identify what is going on and maintain control over the process. This challenge is amplified in a company such as HP that was already complex when it began outsourcing to cloud service providers.

WORKING ACROSS THE BUSINESS

New suppliers need to have up-to-date and formal self-attestation certificates that follow recognized standards, such as Service Organization Controls 2 reports and adhering to the International Organization for Standardization's ISO 27001. To make sure a business division or manager does not randomly contract with a new cloud provider, Brown's team has what he calls a "cast-iron interlock" with procurement. Procurement knows what HP's cloud security requirements are, and they must be included in any new contractual arrangements. In fact, Brown describes the contracts as "living," because they point to the security requirements, which HP can update without changing the actual contract itself.

Working with AWS, HP has created a way of centralizing group security policies through the IT infrastructure. The main cloud instance has all of the group policies established—any new instance sits beneath this "parent" and effectively inherits its security policies automatically. "Every time you make a change to the group policy, it cascades to all the instances that are underneath that," Brown explains. Non-AWS cloud instances go through the new procurement system as described earlier.

As cloud computing becomes synonymous with organizations' IT infrastructures, internal auditors need to work more collaboratively and strategically, according to Scott Shinners, partner of Risk Advisory Services at RSM in Chicago. That will mean audit working increasingly not just with IT and IT security, but with procurement, legal, risk management, and the board.

"The audit committee has to see cloud security in the audit plan, and it also has to be present in the nature of the additional conversations you're having with management," he says. "It should come up not just after implementation, but before in strategy setting and so on." Moreover, if internal audit discovers cloud instances in parts of the business that are not meant to have them, it can feed back to IT and risk management.

Internal audit also needs to work closely with the audit committee as cloud migration, almost inevitably, leads to abandoning a large percentage of the audit plan. "That is where the really good engagement with the audit committee comes through," Shinners says. "How willing is the audit committee to support a trade-off to reduce assurance on moderate risk areas in order to have internal audit spend more

60% of information security professionals say their enterprise's cloud initiatives move faster than their ability to secure them, according to FireMon's State of Hybrid Cloud Security Survey.

of its resources on some of the cutting-edge stuff that is emerging?"

Performing third-party, independent assessments of cloud security and thinking about the underlying controls on data security, access management, breach response plans, and so on, is just the minimum internal audit can do, he says, because that only provides a snapshot in time in a fast-moving area. "The No. 1 way that internal audit can be successful is working with the second line of defense to build a culture around data protection that is pervasive enough to be successful in an environment that is so fast moving," he says. "Making sure risk management gets feedback to know the culture is working is right up internal auditors' alley."

SKILLS AND EXPERTISE

CAEs may also need to reach outside of their organizations to secure audit staff with the right level of skills and qualifications, says Ruth Doreen Mutebe, head of Internal Audit at Umeme, Uganda's largest electricity distributor. She recommends building partnerships with technology and information security institutes, such as ISACA, and universities to help identify good candidates.

"Cloud auditing involves rare skill that takes time to build," she says, especially because it requires people with a good grasp of technical issues who can also communicate those concepts at a basic level to management. In addition to attracting and training staff, a CAE has to be able to retain them after that initial investment has been made.

Mutebe's approach is to recruit a competent IT security auditor—even if a premium price has to be paid—who can effectively audit and guide management on aspects of cloud security. In addition, she encourages her technical staff members to pass on their knowledge to the entire audit team.

"That could include embedding cloud security procedures into what would have been non-IT audits to build capacity and where resources allow, attaching nontechnical internal auditors to support basic tests on cloud security audits," she says. Where gaps remain, outsourcing and co-sourcing arrangements with clearly established service level agreements can be used. "Even there, CAEs should encourage the outsourced service provider to train the internal audit staff," she says.

KEEPING UP WITH CHANGE

Cloud security is moving at a rapid pace, much like other technological changes in businesses today. For internal auditors, that means a focus on critical thinking, learning how to stay current in their industries, and developing a willingness to team up across the business and beyond to form effective alliances. While such an open approach to providing assurance may be new to many auditors working in more traditional environments, it is likely to be a crucial step to take if organizations are to deal with the growing complexity of their cloud initiatives. Ia

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

Cloud migration often leads to abandoning a large part of the audit plan.

"The audit committee has to see cloud security in the audit plan, and it also has to be present in the ... conversations you're having with management."

Scott Shinners

"Cloud auditing involves rare skill that takes time to build."

Ruth Doreen Mutebe

FASTPATH

Automated Cross-Platform Access Controls

The Fastpath Assure® suite is a cloud-based security monitoring, SoD, and compliance platform that can track, review, approve, and mitigate access risks across multiple systems from a single dashboard.

SAP Partner · ORACLE E-BUSINESS SUITE · ORACLE FUSION APPLICATIONS · ORACLE NETSUITE · JDEdwards Enterprise Software

PeopleSoft · Microsoft Dynamics · sage Intacct · Acumatica · workiva

zendesk · Jira Software · coupa · workday · servicenow

Segregation of Duties Analysis

Access Certifications

Audit Trail/ Change Tracking

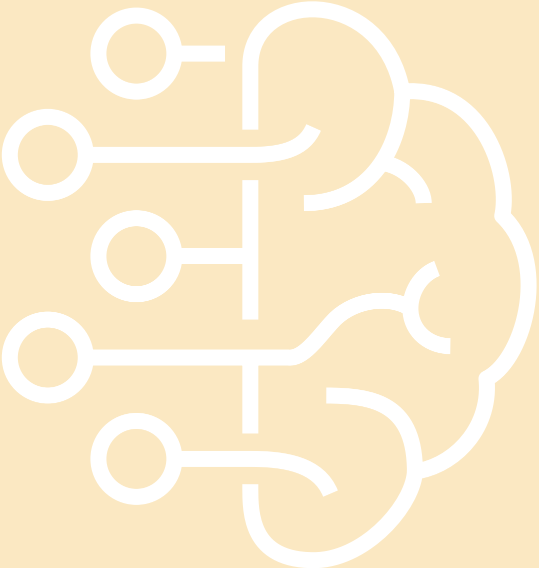
User Provisioning

Emergency Access

Stop by Fastpath Booth #300 at the GRC Conference

Visit gofastpath.com/iia2

Stronger assurance through machine learning



DAVOODA / SHUTTERSTOCK.COM

By inferring from past examples, artificial intelligence tools can generate useful, real-world audit insights.

Ying-Choong Lee

By now, most internal audit functions have likely implemented rule-based analytics capabilities to evaluate controls or identify data irregularities. While these tools have served the profession well, providing useful insights and enhanced stakeholder assurance, emerging technologies can deliver even greater value and increase audit effectiveness. With the proliferation of digitization and wealth of data generated by modern business processes, now is an opportune time to extend beyond our well-worn approaches.

In particular, machine learning (ML) algorithms represent a natural evolution beyond rule-based analysis. Internal audit functions that incorporate ML beyond their existing toolkit can expect to develop new capabilities to predict potential outcomes, identify patterns within data, and generate insight difficult to achieve through rudimentary data analysis. Those looking to get started should first understand common ML concepts, how ML can be applied to audit work, and the challenges likely to arise along the way.

WHAT IS MACHINE LEARNING?

ML is a branch of artificial intelligence (AI) featuring algorithms that learn from past patterns and examples to perform a specific task. How does an ML algorithm "learn," and how is this different from rule-based systems? Rule-based systems generate an outcome by evaluating specific conditions—for example, "If it is raining, carry an umbrella." These systems can be automated—such as through the use of robotic process automation—but they are still considered "dumb" and incapable of processing inputs unless provided explicit instructions.

By contrast, an ML model generates probable outcomes for "Should I carry an umbrella?" by taking into account inputs such as temperature, humidity, and wind and combining these with data on prior outcomes from when it rained and when it did not. Machine learning can even consider the user's schedule for the day to determine if he or she will likely be outdoors when rain is predicted. With ML models, the best predictor of future behavior is past behavior. Such systems can generate useful real-world insights and predictions by inferring from past examples.

> **The outcomes and accuracy of ML algorithms are highly dependent on the inputs provided to them.**

As an analogy, most people who have built objects using a Lego set, such as a car, follow a series of rules—a step-by-step instruction manual included with the construction toys. After building the same Lego car many times, even without written instructions, an individual would acquire a reasonable sense of how to build a similar car given the Lego parts. Likewise, an ML algorithm with sufficient training—prior practice assembling the Lego car—can provide useful outcomes (build the same car) and identify patterns (relationships between the Lego parts) given an unknown set of inputs (previously unseen Lego parts) even without instructions.

COMMON CONCEPTS

The outcomes and accuracy of ML algorithms are highly dependent on the inputs provided to them. A conceptual grasp of ML processes hinges on understanding these inputs and how they impact algorithm effectiveness.

Feature Put simply, a feature is an input to a model. In an Excel table populated with data, one data column represents a single feature. The number of features, also referred to as the dimensionality of the data, varies depending on the problem and can range up to the hundreds. If a model is developed to predict the weather, data such as temperature, pressure, humidity, types of clouds, and wind conditions comprise the model's features. ML algorithms are well-suited to such multidimensional analysis of data.

Feature Engineering In a rule-based system, an expert will create rules to determine the outcome. In an ML model, an expert selects the specific features from which the model will learn. This selection process is known as feature engineering, and it represents an important step toward increasing the algorithm's precision and efficiency. The expert also can refine the selection of inputs by comparing the outcomes of different input combinations. Effective feature engineering should reduce the number of features within the training data to just those that are important. This process will allow the model to generalize better, with fewer assumptions and reduced bias.

Label An ML model can be trained using past outcomes from historical data. These outcomes are identified as labels. For instance, in a weather prediction model, one of the labels for a historical input date might be "rained with high humidity." The ML model will then know that it rained in the past, based on the various temperature, pressure, humidity, cloud, and wind conditions on a particular day, and it will use this as a data point to help predict the future.

Ensemble Learning One common way to improve model accuracy is to incorporate the results of multiple algorithms. This "ensemble model" combines the predicted outcomes from the selected algorithms and calculates the final outcome using the relative weight assigned to each one.

Learning Categories The way in which an ML algorithm learns can generally be separated into two broad categories—supervised and unsupervised. Which type might work best depends on the problem at hand and the availability of labels.

- A *supervised learning* algorithm learns by analyzing defined features and labels in what is commonly called the training dataset. By analyzing the training dataset, the model learns the relationship between the defined features and past outcomes (labels). The resulting supervised learning model can then be applied to new datasets to obtain predicted results. To assess its precision, the algorithm will be used to predict the outcomes from a testing dataset that is distinct from the training dataset. Based on the results of this training and testing regime, the model can be fine-tuned through feature engineering until it achieves an acceptable level of accuracy.
- Unlike supervised learning, *unsupervised learning* algorithms do not have past outcomes from which to learn. Instead, an unsupervised

Among several disruptions facing today's organizations, internal auditors say they are the least prepared and least effective in the area of AI, according to a 2019 Internal Audit Foundation study.

OVERVIEW OF ML PAYMENT ANALYTICS

A payment analytics machine learning model learns well from large amounts of good quality data obtained from diverse sources. Feature engineering selects and weights payment characteristics indicative of high-risk payments. Users then review anomalies identified by the model to determine which, if any, of the payments are inappropriate. Subsequently, the model can learn from the verified data to improve future accuracy.

PAYMENT DATA SOURCES

New and Historical Data

- Payment transaction details
- Human resource data
- Counterparty information
- External risk events
- Emails

MACHINE LEARNING FRAMEWORK

Feature Engineering

- Design features (payment amount, counterparty) to interpret data
- Assign weight to each feature

Machine Learning Algorithms

- Models/algorithms to find outliers and assign risk scores
- Supervised learning through feedback loop to model

USER OUTCOMES

Anomaly Scores

- Data points: transaction amounts and approvers
- High payment anomaly scores

Insights

- Explain features that drive scores
- Active learning: Learning from new user feedback to improve accuracy

learning algorithm tries to group inputs according to the similarities, patterns, and differences in their features without the assistance of labels. Unsupervised learning can be useful when labeled data is expensive or unavailable; it is effective at identifying patterns and outliers in multidimensional data that, to a person, may not be obvious.

STRONGER ASSURANCE

An ML model's capacity to provide stronger assurance, compared to rule-based analysis, can be illustrated using an example of the technology's ability to identify anomalies in payment transactions. "Overview of ML Payment Analytics" on this page shows the phases of this process.

Developing an ML model to analyze payment transactions will first require access to diverse data sources, such as historical payment transactions for the last three years, details of external risk events (e.g., fraudulent payments), human resource (HR) data (e.g., terminations and staff movements), and details of payment counterparties. Before feature engineering work can start, the data needs to be combined and then reviewed to verify it is free of errors—commonly called the extract, transform, and load phase. During this phase, data is extracted from various source systems, converted (transformed) into a format that can be analyzed, and stored (loaded) in a data warehouse.

Next, the user performs feature engineering to shortlist the critical features—such as payment date, counterparty, and amount—the model will analyze. To refine the results, specific risk weights, ranging from 0 to 1, are assigned to each feature based on its relative importance. From experience, a real-world payment analytics model may use more than 150 features. The ability to perform such multidimensional analysis of features represents a key reason to use ML algorithms instead of simple rule-based systems.

Developing an ML model to analyze payment transactions will first require access to diverse data sources.

To begin the analysis, internal auditors could apply an unsupervised learning algorithm that identifies payment patterns to specific counterparties, potentially fraudulent transactions, or payments with unusual attributes that warrant attention. The algorithm performs its analysis by identifying the combination of features that fit most payments and producing an anomaly score for each payment, depending on how its features differ from all others. It then derives a risk score for each

TO COMMENT on this article, EMAIL the author at ying-choong.lee@theiia.org

payment from the risk weight and the anomaly score. This risk score indicates the probability of an irregular payment.

"Payment Outliers" on page 31 illustrates a simple model using only three features, with two transactions identified as outliers. The unsupervised learning model generates a set of potential payment exceptions. These exceptions are followed up to determine if they are true or false. The results can then be used as labels to incorporate supervised learning into the ML model, enabling identification of improper payments with a significantly higher degree of precision.

Supervised learning models can also be used to predict the likelihood of specific outcomes. By training an algorithm using labels on historical payment errors, the model can help identify potential errors before they occur. For example, based on past events a model may learn that the frequency of erroneous payments is highly correlated with specific features, such as high frequency of payment, specific time of day, or staff attrition rates. A supervised learning model trained with these labels can be applied to future payments to provide an early warning for potential payment errors.

This anomaly detection model can be applied to datasets with clear groups, though it should not contain significant transactions that differ greatly from most of the data. For instance, the model can be extended to detect irregularities in almost any area, including expenses, procurement, and access granted to employees.

DEEPER INSIGHTS

Continuing with the payment example, an ML model developed to analyze payment transactions can be used to uncover hidden patterns or unknown insights. Examples include:

- Identify overpayment for services by comparing the mean and typical variance in payment amounts for each product type — such as air tickets or IT services — and highlighting all payments that deviate significantly from the mean.
- Identify prior unknown emerging needs — such as different departments paying for a new service at significantly different prices — or client types by highlighting payment outliers. This insight could allow executives to optimize the cost for acquired products and services.
- Identify multiple consecutive payments to a single counterparty below a specific threshold. This analysis would help identify suspicious payments that have been split into smaller ones to potentially escape detection.
- Identify potential favoritism shown to specific vendors by pinpointing significant groups of payments made to these vendors or related entities.

> **Internal auditors are likely to encounter numerous challenges when applying ML technology.**

KEY CHALLENGES

Internal auditors are likely to encounter numerous challenges when applying ML technology. Input quality, biases and poor performance, and lack of experience with the technology are among the most common.

Availability of Clean, Labeled Data For any ML algorithm to provide meaningful results, a significant amount of high-quality data must be available for analysis. For instance, developing an effective payment anomaly detection model requires at least a year of transactional, HR, and counterparty information. Data cleansing, which involves correcting and removing erroneous or inaccurate input data, is often required before the algorithm can be trained effectively. Experience shows that data exploration and data preparation often consume the greatest amount of time in ML projects. Biases in the training data that are not representative of the actual environment will adversely impact the model's output. Also, without good labels — such as labels on actual cyber intrusions — and feature engineering, a supervised learning model will be biased toward certain outcomes and may generate noisy, or meaningless, results.

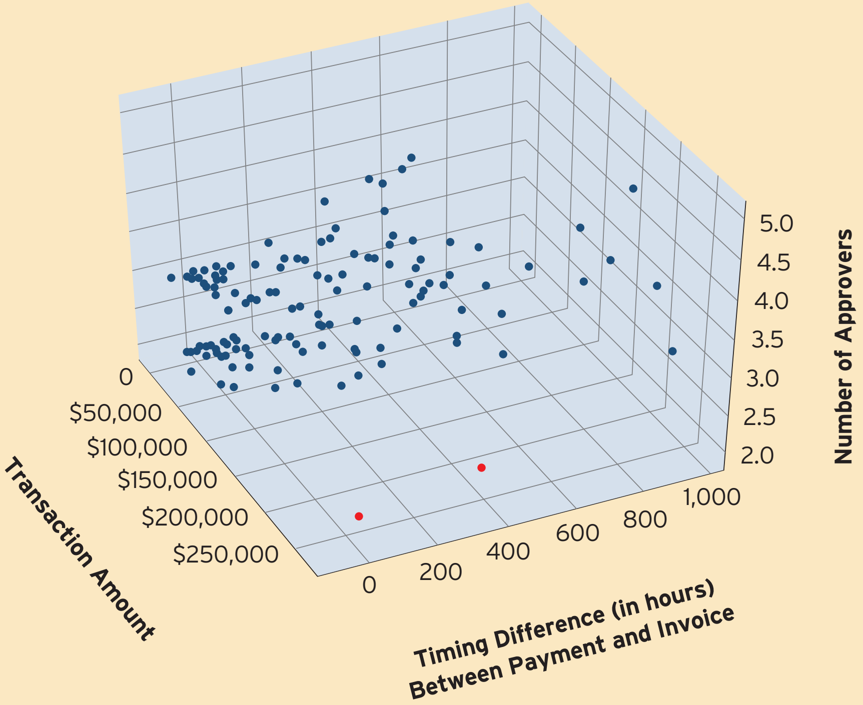
Poor Model Performance and Biases Most internal audit functions that embark on ML projects will initially receive disappointing or inaccurate results from at least some of their models. Potential sources of failure may include trained models that do not generalize well, poor feature engineering, use of algorithms that are ill-suited to the underlying data, or scarcity of good quality data.

Overfitting is another potential cause of poor model performance — and one that data scientists encounter often. An ML model that overfits generates outcomes that are biased toward the training dataset. To reduce such biases, internal audit functions use testing data

MORE **VISIT our mobile app + InternalAuditor.org to view a video series on how AI can help internal auditors assess risk.**

PAYMENT OUTLIERS

By analyzing a set of payment transactions with just three variables, the machine learning model has identified two payment outliers (in red). These payments have significantly higher dollar amounts and fewer approvers compared to all of the others. One payment (bottom-left in red) was also sent out quickly after receipt of the invoice. Both of these outliers could signal inappropriate payment activity.



independent of the training dataset to validate the model's accuracy.

Auditors should also be cognizant of each algorithm's inherent limitations. For example, unsupervised learning algorithms may produce noisy results if the data elements are unrelated and have few or no common characteristics (i.e., no natural groups). Some algorithms work well with inputs that are relatively independent of one another but would be poor predictors otherwise.

Lack of Experience Organizations new to ML may not have examples of successful ML projects to learn from. Inexperienced practitioners can acquire confidence in their fledging capabilities by first applying simple ML models to achieve better outcomes from existing solutions. After these initial successes, algorithms to improve the outcomes of these models can be progressively implemented in stages. For instance, an ensemble learning approach can be used to improve on the first model. If successful, more advanced ML methods should then be considered. This progressive approach can also alleviate the initial skepticism often present in the adoption of new technology.

THE FUTURE OF AUDIT

Machine learning technology holds great promise for internal audit practitioners. Its adoption enables audit functions to provide continuous assurance by enhancing their automated detection capabilities and achieving 100% coverage of risk areas—a potential game changer for the audit profession. The internal audit function of the future is likely to be a data-driven enterprise that augments its capabilities through automation and machine intelligence. Ia

YING-CHOONG LEE, CISA, *is head of IT Audit and Data Analytics, at GIC Private Ltd., in Singapore.*

Wrangling the Intern

The Internet of Things (IoT) allows businesses to connect everything from the office printer to factory production lines via Wi-fi, making it an ideal tool for organizations to exploit, and for employees to use effectively. And there appears to be no limit to what IoT technology is capable of delivering.

Because of how simple it is to install and use the associated software and applications on people's smartphones and tablets, technology heavyweights like Cisco Systems and IT analysts such as Juniper Research estimate that the number of connected IoT devices will reach 50 billion worldwide in 2020. According to research by Forrester, businesses will lead

et of Things

the surge in IoT adoption this year, with 85% of large companies implementing IoT or planning deployments.

But such connectivity comes at a price. As IoT usage increases, so too do the associated risks. Simple devices rely on simple security, and simple protocols can be simply ignored.

A common problem is employees simply adding devices to the network, without informing the IT department—or without the IT team noticing. For example, Raef Meeuwisse, a UK-based cybersecurity consultant and information systems auditor, says that one security technology company revealed that when installing network security detection in new customer networks, it found that up to 40% of devices logged

Connected devices are everywhere in businesses and expanding rapidly, so auditors will have to scramble to ensure they are under control.

Neil Hodge

Illustration by Timothy Cook

on to the network were IoT. "That was a surprise to those organizations' executives and their IT departments," he says.

Such anecdotes mean internal audit has a real job at hand to ensure that IoT deployments go smoothly and that the associated benefits are delivered. And the task is fraught with danger: The technology is still evolving, new risks are emerging, and controls to mitigate these risks often seem to be a step behind what is actually happening in the workplace.

WARNING SIGNS

Information experts and standards-setters such as ISACA point out that because IoT has no universally accepted definition, there aren't any universally accepted standards for quality, safety, or durability, nor any universally accepted audit or assurance programs. Indeed, IoT comes with warning notices writ large. According to ISACA's State of Cybersecurity 2019 report, only one-third of respondents are highly confident in their cybersecurity team's ability to detect and respond to current cyberthreats, including IoT usage—a worrying statistic given the proliferation of IoT devices. Industry experts and hackers have demonstrated how easy it is to target IoT-enabled office security surveillance systems and turn them into spy cameras to access passwords and confidential and sensitive information on employees' computer screens (see "Targeting the IoT Within" on page 35 for examples of other IoT vulnerabilities).

"The use of IoT technology has moved more quickly than the mechanisms available to safeguard devices and their users."

Amit Sinha

"Buying or designing technology before having a clear understanding of the security specification required is a dangerous path."

Raef Meeuwisse

IoT requires organizations to develop their own security specifications.

Distributed denial of service attacks (DDoS) on IoT devices—which analysts and IT experts deem the most likely type of threat—are the best example of IoT device security and governance flaws. In 2016, the Mirai cyberattack on servers at Dyn, a company that controls much of the internet's domain-name infrastructure, temporarily stalled several high-profile websites and online services, including CNN, Netflix, Reddit, and Twitter. Unique in that case was that the outages were caused by a DDoS attack largely made up of multiple, small IoT devices such as TVs and home entertainment consoles, rather than via computers infected with malware. These devices shared a common vulnerability: They each had a built-in username and password that could be used to install the malware and re-task it for other purposes. The attack was the most powerful of its type and involved hundreds of thousands of hijacked devices.

"As is often the case with new innovations, the use of IoT technology has moved more quickly than the mechanisms available to safeguard devices and their users," says Amit Sinha, executive vice president of engineering and cloud operations at cloud security firm Zscaler in San Jose, Calif. "Enterprises need to take steps to safeguard these devices from malware attacks and other outside threats."

BEGIN WITH SECURITY

Events like the Mirai attack make security a priority for internal auditors to review. Among the top IoT security concerns that experts identify are weak default and password credentials, failure to install readily available security patches, loss of devices, and failure to delete data before using a new or replacement device. The steps to rectify such problems are relatively simple, but they are "usually ignored or forgotten about," says Colin Robbins, managing security consultant at Nottingham, U.K.-based cybersecurity specialist Nexor.

As a starter, he says, internal auditors should check that the business has

37% of organizations say a cyberattack on IoT devices compromised customer data, according to the Irdeto Global Connected Industries Cybersecurity Survey.

TARGETING THE IoT WITHIN

In January 2017, the U.S. Food and Drug Administration issued a statement warning that certain kinds of implantable cardiac devices, such as pacemakers and defibrillators, could be accessed by malicious hackers. Designed to send patient information to physicians working remotely, the devices connect wirelessly to a hub in the patient's home, which in turn connects to the internet over standard landline or wireless connections. Unfortunately, technicians found that certain transmitters in the hub device were open to intrusions and exploits. In a worst-case scenario, hackers could manipulate the virtual controls and trigger incorrect shocks and pulses, or even just deplete the device's battery. Manufacturers quickly developed and deployed a software patch.

The case demonstrates the need for internal audit to check that Wi-fi networks are secure, that default factory settings on any connected devices are not used, and that the organization, through the IT department, has patch management processes in place to check whether any devices have security updates that need to be installed.

a process to ensure that all IoT device passwords are unique and cannot be reset to any universal factory default value to minimize the risk of hacking. The organization should update software and vulnerability patches regularly, and devices that cannot be updated—because of age, model, or operating system—should be isolated once personal and work data has been removed from them.

"Organizations need to have conversations at the highest level of management about what IoT means to the business," says Deral Heiland, IoT research lead at Boston-based cybersecurity firm Rapid7. Once they have done this, Heiland suggests they focus on detailed processes around security and ask key questions such as: What IoT has the organization currently deployed? Who owns it? How does the organization manage patches for these technologies, and how does it monitor for intrusions? What processes does the organization need for deploying new technologies?

TECHNICAL HYGIENE STANDARDS

Effective IoT security requires organizations to develop their own protocols and security specifications up front, Meeuwisse says. This ensures that "devices can either be integrated into particular security zones or quarantined and excluded from the possibility of getting close to anything of potential value," he explains.

Meeuwisse adds that whether a business is manufacturing or simply installing IoT devices, having security architecture standards to ensure information security throughout the organization is aligned with business goals is a crucial first step. "Buying or designing technology before having a clear understanding of the security specification required is a dangerous path," he says. "For any new type of IoT device, there should always be a risk assessment process in place to understand whether the device meets security requirements, needs more intensive scrutiny, or poses a significant potential risk."

More widely, organizations need to examine "the basics" to ensure that they maintain their IT system's "technical hygiene," says Corbin Del Carlo, director, internal audit IT and infrastructure at financial services firm Discover Financial Services in Riverwoods, Ill. For example, Wi-fi access should be closed so only authorized and certified devices can use it, and there should be an inventory of devices that are connected to the network so the IT department knows who is using them. For additional security, IT should scan the network routinely—even daily—to check whether new devices have been added to the network and whether they have been approved.

Del Carlo also says internal auditors need to check that the organization's IT architecture can support a potentially massive scale-up of devices wanting to access its systems and network quickly. "We're talking about millions more devices all coming online within a year or two," he says. "Can your IT system cope with that kind of increase in demand? What assurance do you have that the system won't fail?"

Del Carlo recommends organizations draw up a shortlist of device manufacturers that are deemed secure enough and compatible with their IT architecture. "If you allow devices from any manufacturer to access the network, then you need the in-house capability to monitor the security of potentially hundreds of different makes and find security patches for them all, which can be very time-consuming," he points out.

A list of approved manufacturers also can make it easier to audit whether

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

the devices have the latest versions of security downloads. "Even if a particular manufacturer's product proves to have vulnerabilities, it is much easier to fix the problem for all those devices than try to constantly monitor whether there are security updates for many different products made by dozens of manufacturers," he says.

INTRUSIVE MONITORING

It's not only the organization's security that internal auditors should consider. Auditors also should make management aware of potential privacy issues that some applications may present—especially those that feature GPS tracking, cameras, and voice recorders. "Tracking where employees are can be useful for delivery drivers, but is it necessary to track employees who are office-based?" Del Carlo asks.

An example is an IoT app that monitors how much time people spend at their desks and prompts them to take a break if they are there too long. Organizations could use that technology to monitor how frequently people are not at their desks, Del Carlo notes. "While this may catch out those who take extended lunch breaks, it may also highlight those who have to take frequent trips to the bathroom for medical conditions that they may wish to keep private," he explains. "As a result, auditors should query such device usage."

BUSINESS RISKS

Yet while there is a vital need to make IoT security a priority, Robbins says organizations should not overlook whether management has appropriately scoped the business case for an IoT deployment, and how success or failure can be judged. "As with any other project, particularly around IT, managers can throw money at something they do not understand just because they think they need it, or because everyone else is using it," he says.

Robbins cautions that poorly implemented IoT solutions create new vulnerabilities for businesses. "With IoT, it's not data that is at risk, but business processes at the heart of a company," he points out. "If these processes fail, it could lead to a direct impact on cost or revenue."

According to Robbins, the success of IoT means a heavy—and "almost blind"—reliance on the rest of the "things" that support the technology working effectively within the supply chain. Take for example an IoT device that monitors bakery products made in an oven. That device may tell the operator that the oven temperature is 200 degrees and the baked goods have another 20 minutes of cooking time, he explains.

"But the problem is that you have no physical way of checking, or even being alerted, that the technology might be wrong or has been hacked, and that the settings and readings are incorrect," Robbins says. "Everyone is relying on all the different parts of the supply chain—the app vendor, the cloud provider, and so on—maintaining security in a world where there are no agreed-upon standards or best practice. Talk about 'blind faith.'"

IoT also increases the need for additional third-party and vendor risk monitoring, Del Carlo warns. This is because app developers not only may be collecting data from users to help inform design improvements but also to generate sales leads.

"Internal auditors need to think about the data that these vendors might be getting and how they may be using it," Del Carlo explains. For example, developers may be exploiting user data to approach the organization's competitors with products tailored to the competitor's needs. "Internal auditors need to check what data developers may be collecting and why," he advises.

"Organizations need to have conversations at the highest level of management about what IoT means to the business."

Deral Heiland

"With IoT, it's not data that is at risk, but business processes at the heart of a company."

Colin Robbins

Large enterprises spent an average of $4.6 million on IoT in 2018 and 86% plan to increase IoT spending this year, Zebra Technologies' Intelligent Enterprise Index reports.

EARLY BEST PRACTICES

Despite the absence of universally agreed-upon guidance for aligning IoT usage with business needs, some industry bodies have tried to promote what they consider to be either basic steps or best practice. For instance, in a series of blog posts, ISACA recommends that organizations perform pre-audit planning when considering investing in IoT solutions. It advises organizations to think about how the devices will be used from a business perspective, what business processes will be supported, and what business value is expected to be generated. ISACA also suggests that internal auditors question whether the organization has evaluated all risk scenarios and compared them to anticipated business value.

Eric Lovell, practice director for internal audit technology solutions at PwC in Charlotte, N.C., says internal audit should have a strong role in ensuring that IoT risks are understood and controlled, and that the technology is aligned to help achieve the organization's business strategy. "Internal audit should ask a lot of questions about how the organization uses IoT, and whether it has a clear strategic vision about how it can use the technology and leverage the benefits from it," he says.

As IoT is part of the business strategy, Lovell says internal auditors need to assess the business case for it. "Internal auditors need to ask management about the business benefits it sees from using IoT, such as improving worker safety, better managing assets, or generating customer insights, and how these benefits are going to be measured and assessed to ensure that they have been realized," he advises.

Questions to ask include: What metrics does the organization have in place to gauge success or failure? Are these metrics in line with industry best practice? Are there stage gates in place that would allow the organization to check progress at various points and make changes to the scope or needs of the project? "Equally importantly, does the organization have the right people with the necessary skills, experience, and expertise to check that the technology is delivering its stated aims and is being used securely?" Lovell notes.

Lovell also says internal auditors need a seat at the table from the beginning when the organization embarks on an IoT strategy. "Like with any other project, internal audit will have less influence and input if the function joins the discussion after the project has already been planned, scoped, and started," he explains. "Internal auditors need to make sure that they are part of those early discussions to gauge management's strategic thinking and their level of awareness of the possible risks and necessary controls and procedures."

IOT'S DYNAMIC RISKS

Risks shift over time as technology innovations and the business and regulatory environment evolve. "It is pointless to think that the risks that you have identified with IoT technologies at the start of the implementation process will remain the same a couple of years down the line," Lovell says. "Internal auditors need to constantly review how IoT is being used—and under what circumstances and by whom—and assess whether the technology is still fit for purpose to meet the needs of the business." Ia

What metrics does the organization have to gauge success or failure?

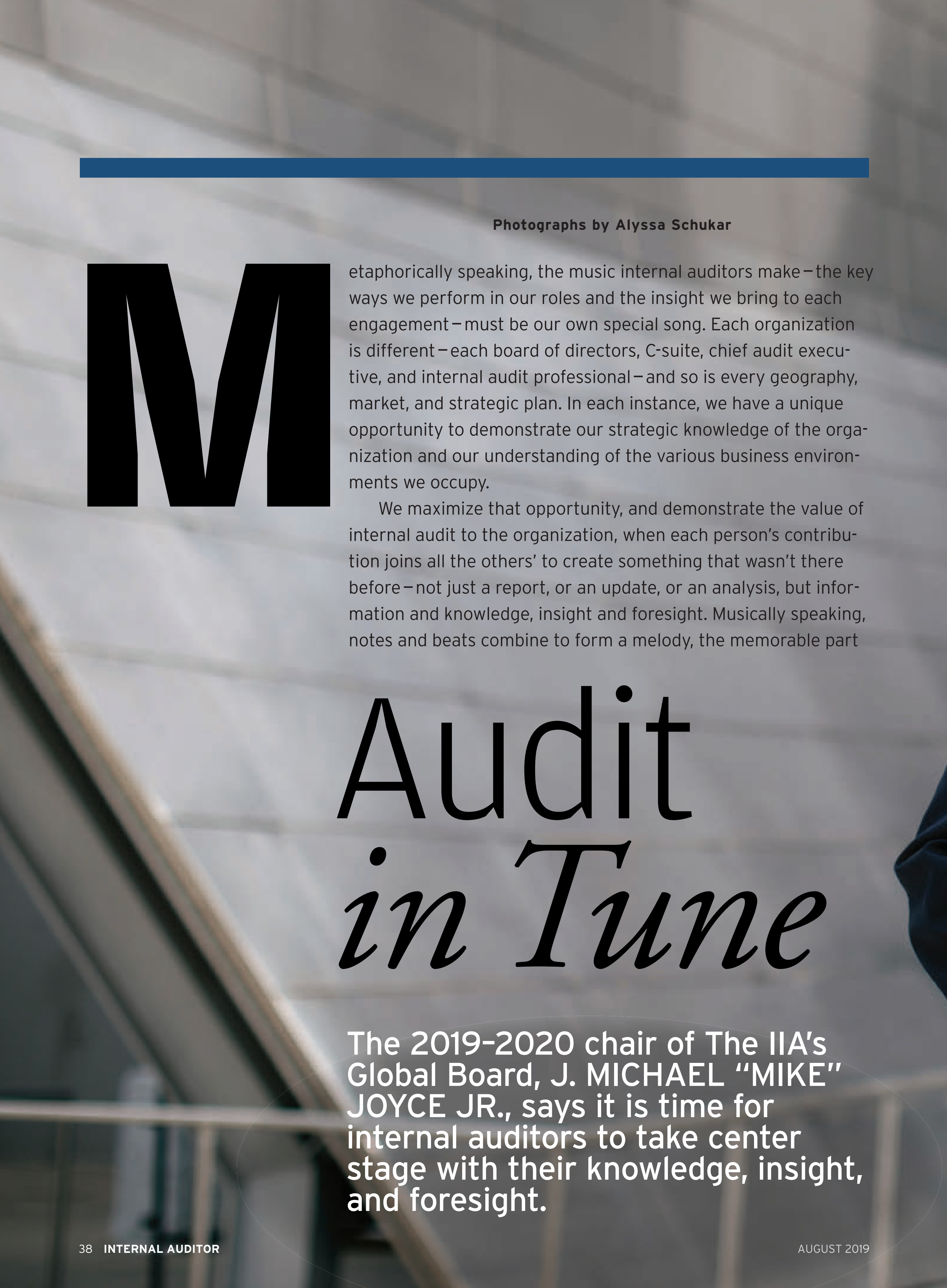
NEIL HODGE *is a freelance journalist based in Nottingham, U.K.*

"Internal auditors need to think about the data that these vendors might be getting and how they may be using it."

Corbin Del Carlo

"Internal audit should ask a lot of questions about how the organization uses IoT, and whether it has a clear strategic vision about how it can use the technology."

Eric Lovell



Photographs by Alyssa Schukar

Audit *in Tune*

The 2019–2020 chair of The IIA's Global Board, J. MICHAEL "MIKE" JOYCE JR., says it is time for internal auditors to take center stage with their knowledge, insight, and foresight.

Metaphorically speaking, the music internal auditors make—the key ways we perform in our roles and the insight we bring to each engagement—must be our own special song. Each organization is different—each board of directors, C-suite, chief audit executive, and internal audit professional—and so is every geography, market, and strategic plan. In each instance, we have a unique opportunity to demonstrate our strategic knowledge of the organization and our understanding of the various business environments we occupy.

We maximize that opportunity, and demonstrate the value of internal audit to the organization, when each person's contribution joins all the others' to create something that wasn't there before—not just a report, or an update, or an analysis, but information and knowledge, insight and foresight. Musically speaking, notes and beats combine to form a melody, the memorable part

IIA GLOBAL BOARD CHAIR

MORE VISIT our Mobile App + InternalAuditor.org to watch the 2019-20 Chairman's Video.

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

of a song that stays in our heads because it's catchy, or moving, or somehow more engaging than usual. Our internal audit melody consists of the advice, data, and background details we provide that contribute to the organization's success.

Of course, melody without harmony can seem detached and less relevant—and melody without rhythm can ramble without direction or emphasis. Music is most memorable when all the elements are in sync. Our input as internal auditors is much the same. When we *Audit in Tune*, my theme as the 2019–2020 chair of The IIA's Global Board, we combine our growing influence and our ongoing grasp of the fundamentals of the profession.

FINE-TUNING INTERNAL AUDIT

Successful audit professionals continuously fine-tune their audit approach and philosophy to adjust to rapidly changing conditions and to account for the evolving expectations of their stakeholders, whether we are auditing a business; a nonprofit organization; a university or school system; or a local, county, regional, state, or federal government entity.

As our influence and authority within our organizations continues to grow, we serve our stakeholders best, and keep earning our seat at the table, by building collaborative relationships with management and all other departments, including finance, IT, human resources, and legal, that help facilitate review and mitigation of key risks. I cannot overemphasize the specific merits of strong relationships with the organization's compliance function, if it's separate from internal audit. There's mutual benefit in working together to identify risk management opportunities that may not be evident to either function alone.

Indeed, our value proposition as internal auditors is built on maintaining a voice—and ongoing strong rapport and visibility—with the audit committee and senior management, and reinforcing the professional and standards-driven orientation of the function. That's what helps foster a corporate culture where our contributions are understood and respected. Forming and keeping those internal ties can be as simple a proposition as scheduling periodic lunches or meetings with relevant personnel; just about any format for keeping in touch will work, as long as it upholds the organization's cultural standards and the internal audit function's independence.

This is critical: We don't have to sacrifice our objectivity to successfully partner with our clients. Indeed, some of the best, most useful audit observations come from colleagues—the board, C-suite, line management, or hourly employees—who trust us.

PROVIDING THE MELODY

For internal auditors to provide the melody behind their organization's success, they need the right instruments. That's where The IIA comes in. Ultimately, it is The IIA's responsibility to provide internal auditors with the information they need in advance—before challenges grow too large—so they can then provide real value and unique insights to their own stakeholders.

Challenging times loom, and The IIA stands ready to help internal

The CIA reflects our commitment to continued professional growth.

auditors face them with streamlined organizational governance as nimble and flexible at the global level as individual internal auditors must be every day. When internal auditors turn to The IIA for support and assistance, The Institute must respond quickly with the required updates and details. Beginning two years ago, The IIA embarked on a comprehensive assessment of its own governance practices, benchmarking as it progressed against a wide variety of resources. Two of the key outcomes of that review were a significant reduction in the size of the Global Board—from 38 members to 17—and elimination of the 10-member Executive Committee of the Board. In a sense, the entire 17-member new Board will function as an Executive Committee. Those changes were approved by the membership in May 2018, and they became effective with our Annual Business Meeting in July 2019.

Moving forward, one of the many expected outcomes of the change to a leaner, more-laser-focused approach will be a more nimble decision-making process at The IIA's Global Headquarters, so it can respond to emerging issues more timely, while maintaining a focus on the strategic issues involved in operating an enterprise this large. This enables the Board to provide forward-thinking guidance both to the organization and to the organization's members.

The IIA's reorganization and ongoing efforts are designed with rhythm and harmony in mind, too, of course. They're the other elements—"rhythm" is developing our skills at performing the basic functions of our profession, and "harmony" is expanding contact and colleague networks within our organizations—that combine with "melody" to create the music internal auditors make when they audit in tune.

ACHIEVING HARMONY

In music, harmony is achieved with chords that move from beginning to middle to end, combining individual notes into richer, deeper sounds that blend multiple individual sonic expressions to tell a more impactful musical story. In internal auditing, harmony is the influential role auditors play in our organizations' success. Internal audit needs to be in lockstep with all of our

In music, harmony can come from a musical instrument or an orchestra, a voice or a choir. And if we audit in tune, the music we make can come in any format, as long as the right content is there.

stakeholders—and manage our audit processes in a way that's structured to hold everything together. That enables auditors to identify the key risks facing our organizations and ensure that our audits are timely, relevant, and responsive. This includes providing useful, meaningful advice on mitigating and exploiting those key risks, as appropriate.

At my organization, the Blue Cross Blue Shield Association, we're fortunate to operate in an environment with a strong ethics and control culture that supports the work we do—and that facilitates collaboration among colleagues with shared goals and interests. You might say we operate in a "harmonious" environment.

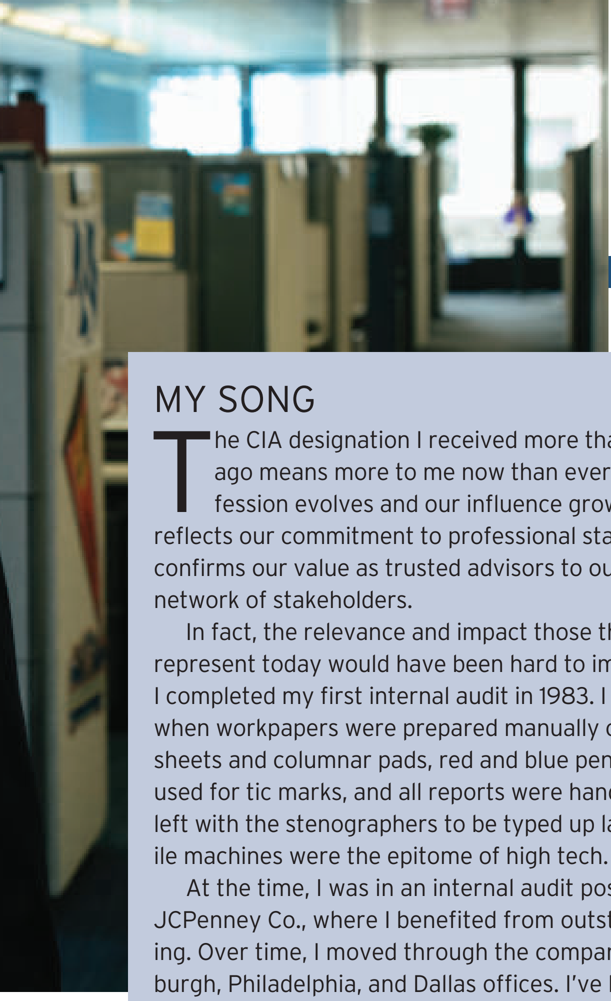
In music, harmony can come from a musical instrument or an orchestra, a voice or a choir. And if we audit in tune, the music we make can come in any format, as long as the right content is there. For example, when it comes to documenting our work, it doesn't matter whether our instrument of choice is a simple desktop application or a vendor-supplied workpaper tool—nor whether you're a solo act or part of the 100-plus member London Philharmonic Orchestra. At the end of the day, we all need efficient, professional, clear, and objective techniques to validate and support our audit observations and recommendations.

THE RHYTHM OF THE IPPF

The techniques internal auditors use, no matter how sophisticated, must be based on the basics of our profession. Every piece of music has a backbone of rhythm—it's the building block that supports a song. Similarly, when I talk about rhythm as part of my theme this year, I'm referring to internal audit's need to master and employ the fundamentals of the field as the processes we use, and the stakeholders we serve, continue to evolve. Indeed, as stakeholder expectations increase for many internal audit departments, we need to remember that credibility—one of our most valuable qualities—comes from both current knowledge and command of the basic skills that define a profession.

Demonstrating our command of the critical fundamentals of our work begins with the implementation of the International Professional Practices Framework (IPPF). The IPPF really should underpin everything we do as we engage in frequent and robust discussions with our audiences—our boards and audit committees, senior and operating managers, and, importantly, regulators. Consider the IPPF's Code of Ethics and *International Standards for the Professional Practice of Internal Auditing* to be the sheet music from which we should all be playing. The functions it facilitates—our ability to proactively identify and prioritize corporate risks, maximize finite audit resources through efficient and innovative audit techniques, and develop value-added recommendations for enhancing operations to help management achieve its objectives—are tangible metrics internal auditors can demonstrate.

I'm also a relentless advocate for professional certification. Becoming more complete internal auditors requires us to support the Certified Internal Auditor (CIA) designation, a globally recognized symbol



of professionalism that demonstrates our ability to play a leading role in elevating organizational success. The CIA reflects our commitment to continued professional growth and development and shows our value as trusted advisors. Truly, it plays an instrumental role in helping us make our mark on our organizations and our profession.

A BRAND NEW BEAT

We have the opportunity to maximize our results when we audit in tune. Enhancing our rhythms, harmonies, and melodies will be increasingly critical in the future. The key challenges we face—remaining relevant and increasing our value to stakeholders, given the pace of innovation and changing risks; providing consistent work product quality, given the varying maturity of the function globally; and the continuing need to increase our skills—will demand every resource we can command in response.

It's time for internal audit to move to a new beat—each department's and each practitioner's unique blend of industry insight and strategic smarts—in every geography The IIA represents. And it's time to take center stage for broader and broader audiences. But as we do so, we can't forget our fundamentals. Let's take on the challenges ahead as a band of professionals making our own kind of music.

J. MICHAEL "MIKE" JOYCE JR., CIA, CRMA, CPA, *is vice president, chief auditor and compliance officer at Blue Cross Blue Shield Association in Chicago.*

MY SONG

The CIA designation I received more than 30 years ago means more to me now than ever. As our profession evolves and our influence grows, the CIA reflects our commitment to professional standards and confirms our value as trusted advisors to our growing network of stakeholders.

In fact, the relevance and impact those three letters represent today would have been hard to imagine when I completed my first internal audit in 1983. I remember when workpapers were prepared manually on narrative sheets and columnar pads, red and blue pencils were used for tic marks, and all reports were handwritten and left with the stenographers to be typed up later. Facsimile machines were the epitome of high tech.

At the time, I was in an internal audit position with JCPenney Co., where I benefited from outstanding training. Over time, I moved through the company's Pittsburgh, Philadelphia, and Dallas offices. I've been with the Blue Cross Blue Shield Association (BCBSA) in Chicago since 1999, where I serve as the vice president, chief auditor and compliance officer. BCBSA is a national association of 36 independent, community-based, and locally operated companies that together cover more than 107 million members.

The scope of my internal audit work includes our Chicago and Washington, D.C., offices. We build an annual plan as a guide for addressing identified risks and then adjust it as necessary. Interestingly, many of the audits come in the form of management requests, which I consider validation that management perceives the value of our services. As compliance officer, I administer our internal code of conduct, business ethics training, conflict of interest process, and compliance helpline, and I am responsible for our national anti-fraud department, which supports the Special Investigation Units battling health-care fraud at each of the Blue Cross Blue Shield licensees. It is important to note that transparent and mitigating controls have been long established to maintain the independence of our internal audit function, despite these "second line of defense" responsibilities.

I was encouraged to volunteer for the IIA–Dallas Chapter shortly after becoming an IIA Audit Group member in 1989. Since my first committee assignment, I've filled an almost unbroken string of committee, officer, and local board roles, including serving as the IIA–Chicago chapter president and on various international and North American committees and assignments. I was the 2015-2016 chair of The IIA's North American Board, which oversees all IIA operations in the U.S., Canada, and the Caribbean. During my term, we went through an intensive strategic planning session to make sure we synched appropriately with The IIA's revised Global Strategic Plan.

The IIA's Global Board–the governing body of The Institute–also has undergone a recent strategic refresh, and we're better equipped than ever to manage The IIA, itself, and to provide the guidance and information that individual chapters and affiliates, as well as individual practitioners, count on us for every day. Our longstanding motto is Progress Through Sharing. My theme is Audit in Tune. I hope that when you combine those messages, what emerges is an orchestra of internal audit professionals helping each other achieve world-class results. Let's have a great year.

An Exclusive
Opportunity

Internal auditors can find the blind spots that have given financial firms a reputation for bad behavior toward customers.

Auditing Conduct

Anders Land

Outrageous behavior by employees within the global financial services industry have put boards and regulators on high alert regarding whether their companies are acting in the best interest of their customers. Recent scandals include Wells Fargo's cross-selling program, where employees were pressured to open new bank accounts and issue credit cards for customers without their knowledge. At Australia's Commonwealth Bank, some financial advisors charged clients service fees even when there was not any record of services being provided. The fallout from these and other scandals has included massive dismissal of staff, millions of dollars in fines, loss of customer confidence, and reputational damages.

Successful financial services companies view their customers as the heart of their business. These companies are focused on the continuous delivery of quality products and services that produce a fair and suitable outcome for their customers. Regulators and corporate boards expect companies to measure and demonstrate appropriate conduct toward their customers. Inappropriate, unethical, or unlawful behavior by the organization's management or employees that lead to poor customer outcomes is not acceptable.

Today, conduct issues pose a great risk to a company's success and sustainability. In addition to regulatory fines, companies that do not mitigate conduct

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

issues may face a quick trial by "word of mouth" in social media that could result in reputational damage and loss of trust. It may be nearly impossible for an organization to manage the crisis and respond timely to correct the misconduct once the story gains traction on social media. That's why internal audit departments should play a significant role in assessing whether their organization's conduct risk framework is fit for purpose and identifies potential blind spots that management needs to address.

CONDUCT CHALLENGES

The main challenge for internal auditors is that each organization's conduct risk profile is unique and there is no "one size fits all" prescribed framework for assessing behaviors toward customers. As a result, there is no standardized approach to auditing conduct risk. As large financial services organizations operate in multiple jurisdictions, with different legal and regulatory environments, the ability to design an audit program that can depict a timely and holistic view of conduct becomes complex.

> A challenge in assessing conduct risk is that public sentiment and societal norms are constantly evolving.

Another challenge in assessing conduct risk is that public sentiment and societal norms are constantly evolving. What was considered acceptable behavior in the past may be viewed differently today. For example, in the past it was considered acceptable to smoke in the workplace, but today smoking in offices is viewed as unacceptable and is illegal in many places.

Similarly, in the financial services industry, the adoption of technology and democratization of information have dramatically changed what are considered acceptable fees to charge for mutual funds. Average mutual fund fees or expense ratios have declined substantially over the past 20 years from in excess of 1% in 1996 to a fraction of a percent in 2019. Auditors need to understand not only their organization's operations intimately, but also the regulatory and societal expectations.

To evaluate whether an organization is acting with integrity in dealing with its customers, internal audit should assess whether the business designs and sells products and services in the best interest of the customer. As culture and conduct risks are interconnected, auditors should consider multiple factors that drive conduct and behaviors, including:

- Corporate governance.
- Remuneration.
- Incentive schemes.
- Product development.
- Sales practices.
- Fees and charges.
- Customer service.
- Complaints handling.
- Training.

In general, a strong customer-focused culture leads to fewer conduct failings and helps to mitigate conduct risk. Internal auditors should leverage any previous audit work covering corporate governance, culture, and ethics in their conduct assessment. They should align their audit approach to the scale, business model, complexity, geographical reach, and regulatory environments in which the organization operates. Auditors should provide assurance on the design and effectiveness of controls over conduct risks and determine whether the controls in place are adequate and effective to mitigate the risk of poor customer outcomes.

Financial services companies allocate 4.5% of their audit plan to culture and governance versus 2.9% for publicly traded firms, The IIA's 2019 North American Pulse of Internal Audit reports.

CONDUCT AUDIT TIPS

Effective mitigation of conduct risk looks beyond mere compliance with laws and regulations while putting the customer's interests first. Auditors charged with assessing conduct risk within an organization should:

- Avoid a "check-the-box" approach.
- Be customer-outcome focused by looking at behaviors from the customer's perspective. For example, in looking at a product offering, auditors should ask whether the company did right by the customer.
- Go beyond regulation to call out detrimental conduct risk that is embedded in the organization's strategy, values, and culture.
- Don't just focus on "hard" controls. Auditors should look at soft controls that can give them a feel for how business is conducted outside the formal audit program. For example, does the culture encourage employees to meet aggressive or unrealistic sales targets?
- Seek specialist knowledge from external experts if the organization lacks such expertise in-house.
- Emphasize reporting and data analytics to identify potential conduct blind spots.

AUDIT OPTIONS

In developing a structured approach to systematically assess conduct risk, auditors need to determine whether a top-down, bottom-up, end-to-end, or integrated audit is best suited for their organization. Regardless of what approach auditors select, the organization's conduct risk framework is key. This framework should be anchored around the organization's business strategy, risk appetite, culture, and values.

Top-down The top-down audit approach starts by assessing the adequacy of an organization's conduct risk framework and how the framework translates into policies. Then it drills down into how existing processes and controls over governance, risk appetite, culture, and behavior mitigate conduct risks.

Bottom-up In the bottom-up audit approach, auditors assess the processes and controls within a business unit to determine whether conduct risk is mitigated. Auditors then can aggregate the conduct risk results of each audit into a thematic paper for effective communication to the board and senior management.

End-to-End This audit approach evaluates the customer interaction value chain in its entirety. The customer interaction value chain comprises:

- Product design.
- Pricing.
- Distribution.
- Sales practices.
- Claims handling.
- Complaints.

While comprehensive, drawbacks to this approach are the manpower

> **The conduct risk framework should be anchored around the business strategy, risk appetite, culture, and values.**

Crowe

Blockchain and Internal Audit

Blockchain networks are growing in popularity. With its potential to transform business processes, how should the internal audit profession respond? The Internal Audit Foundation, in collaboration with Crowe, and with the support of The Institute of Internal Auditors' Audit Executive Center, has published "Blockchain and Internal Audit." This joint research report provides internal auditors with a basic framework for assessing current levels of blockchain technology preparedness and a road map for developing audit plans that address blockchain issues as they are encountered.

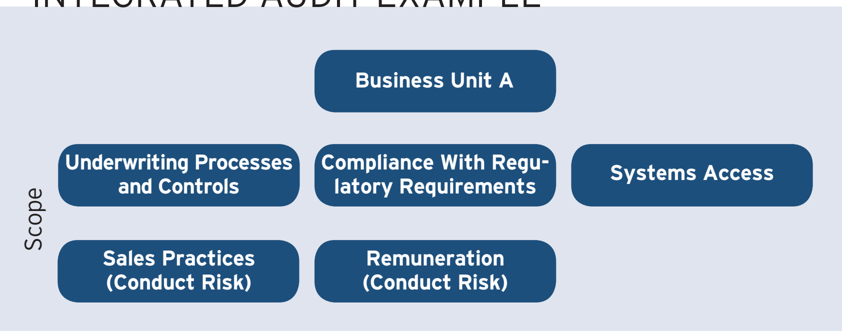
To read the full report, visit: **lp.crowe.com/bcia**

IIA PRINCIPAL PARTNER

CC2015-001H

Employees are 11 times more likely to report misconduct when the business proactively communicates about ethics, The Ethics & Compliance Initiative's 2018 Global Business Ethics Survey notes.

INTEGRATED AUDIT EXAMPLE


Business Unit A
Scope
Underwriting Processes and Controls
Compliance With Regulatory Requirements
Systems Access
Sales Practices (Conduct Risk)
Remuneration (Conduct Risk)

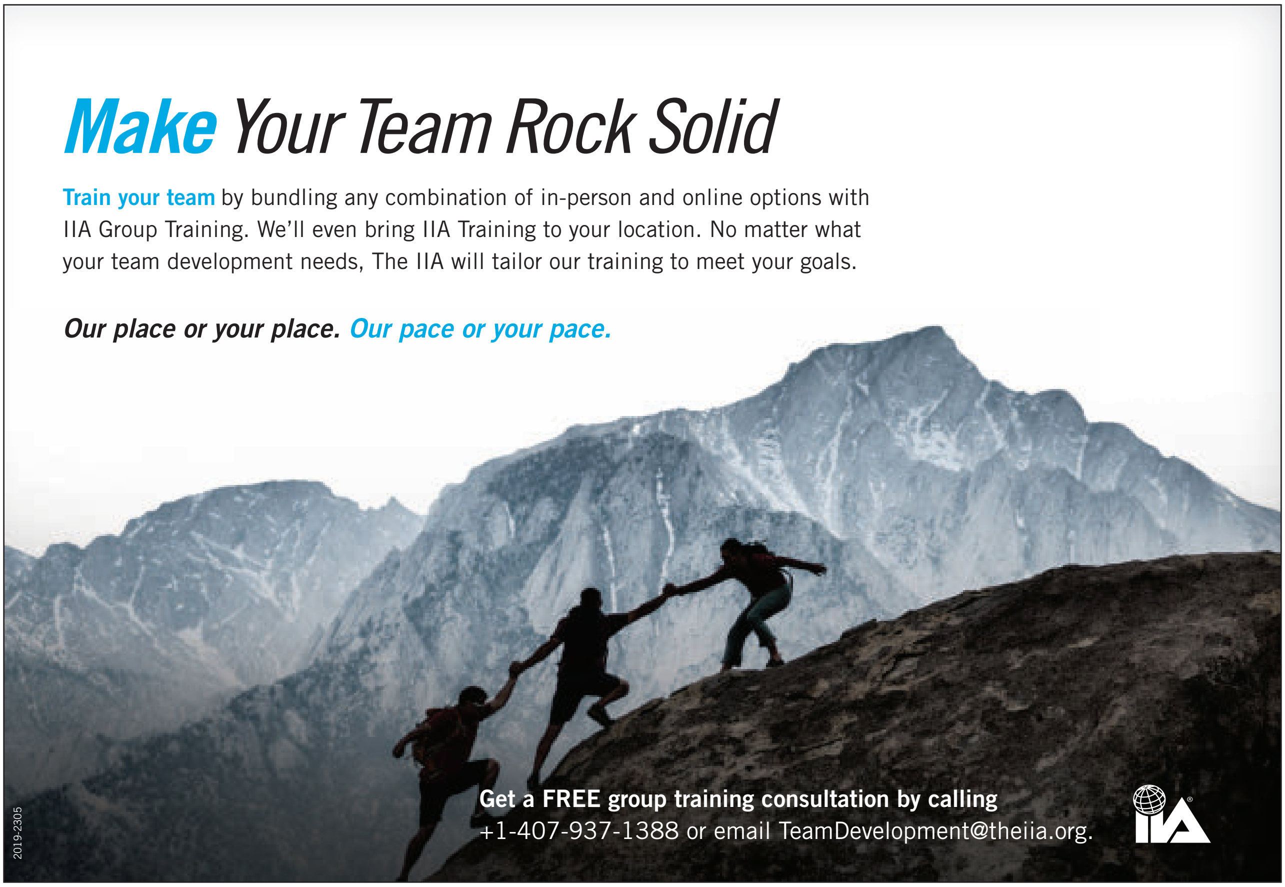
necessary to complete the audit and potential untimely communication of any findings.

Integrated In the integrated audit approach, internal auditors consider aspects of conduct risk in every audit of a business unit (see "Integrated Audit Example," this page). Such audits can range from an evaluation of sales practices during an underwriting audit to looking at incentive schemes and training programs during a regulatory compliance audit. Auditors would report any conduct risk findings as an issue in each applicable audit.

CONDUCT BLIND SPOTS

Internal audit's holistic view of an organization positions the department to identify potential conduct risk blind spots by assessing the organization's underlying culture and conduct toward customers. Moreover, in their advisory role, auditors can highlight specific departments and individuals as role models whenever they find exemplary behavior and best practices in conduct risk mitigation. These actions can help ensure the organization's conduct stays on the straight and narrow. Ia

ANDERS LAND, CFE, *is group head of internal audit and chief audit executive at QBE Insurance Group in New York.*



POSTERIORI / ISTOCK.COM

A Blended Approach

Active auditing—combining Lean and Agile techniques—can drive down wasted time and transform the auditor–client relationship.

Prescott Coleman
Sandra Kasahara

Traditional audits are often awash in wasted time, unnecessary conflict, and incorrect assumptions. Active auditing is a form of Agile auditing that was developed in a major utility company to eliminate, or at least substantially decrease, these kinds of wasteful activities. The term active auditing was, in fact, coined because it is the antonym of passivity and waiting.

Lean—often synonymous with the Toyota Production System—is a change-making methodology. Agile is an IT project management approach. Active auditing borrows concepts from both disciplines to create a more efficient way to run audits. The catalog of material describing both Lean and Agile principles is vast, so active auditing borrows only what is needed to create an audit system that can work better than a traditional one. The system can best be explained by breaking it down into three pillars.

PILLAR ONE: ENERGETIC COLLABORATION

Lean and Agile both preach that there can be only one team, and that team members must work together throughout the project. However, the reality is often two teams—the audit client and auditors—facing each other across a battlefield even while proclaiming their intent to work collaboratively. Active auditing recognizes that both teams work for the board, and the board has the right

to expect both to behave as a single, combined team.

Collaborating energetically is a choice to which both auditors and audit clients must commit. Without deliberate and overt commitment, both groups tend to fall back into bad habits. Once committed, the two develop shared ground rules—defining what's nonnegotiable for each of them and how they want to work together. Personal connection is critical for collaboration, so information should be shared early, often, and in person, as much as possible.

Auditors must be the first to extend an authentic, though likely uncomfortable, hand to the audit clients to collaborate. And they must mean it.

Beyond the practical steps, auditors must lead in making themselves open and vulnerable. This can be a scary step, as auditors typically are so accustomed to maintaining professional distance that laying their cards on the table may not come naturally. Auditors must be the first to extend an authentic, though likely uncomfortable, hand to the audit clients to collaborate. And they must mean it—in everything they say and do.

When teams energetically collaborate, better information is offered, rather than extracted; far less time is wasted; there are fewer misunderstandings; clients grow to believe the auditors understand them; there is less conflict, which is good for clients and auditor; and the audit can be fun.

TO COMMENT on this article, **EMAIL the authors at prescott.coleman@theiia.org**

PILLAR TWO: ITERATIVE AUDIT EXECUTION

Agile as a software development methodology was created to counter traditional sequential Waterfall techniques. Waterfall is how most construction projects are managed—by planning, designing, building, and implementing. It relies on high-quality requirements-gathering at the beginning of a project and an acceptance that changes midstream are unwelcome. In contrast, Agile embraces flexibility and change. To manage this flexibility, Agile breaks the work down into iterations, or sprints. An iteration is a mini-software project, with a specified beginning and end, that is structured to produce working and sellable software at its completion. If a typical large software project takes two years, an Agile project will produce perhaps 12 instances of sellable code over that time, whereas a Waterfall project will produce one.

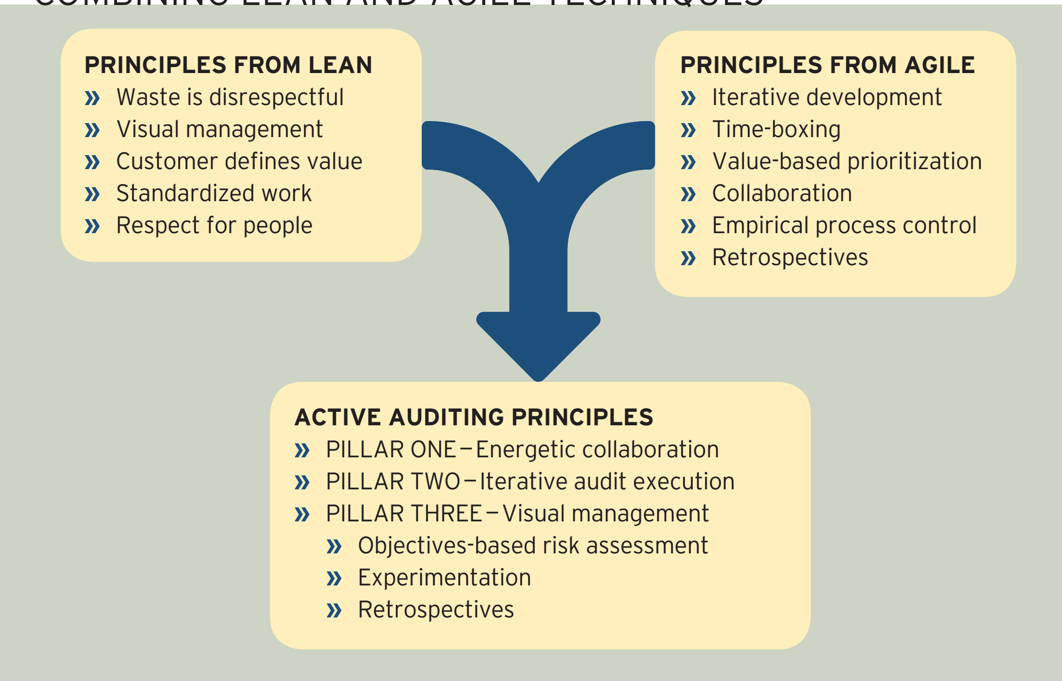
The overall risk of the project is reduced because the Agile project tests the market frequently, while the Waterfall project hopes its grand unveiling two years from now is still what the market wants.

Active auditing borrows from the concept of iterations—breaking down the audit program into mini-audits. The typical steps of an audit—from risk assessment to workpaper approval—still occur, but in smaller chunks. And they are completed before moving to the next iteration.

Active auditing starts by building an overall audit program, which is the best initial guess at the right control objectives and fieldwork steps. Then, using engagement planning sessions, the work is assigned to time-boxed iterations. Time-boxing establishes start and end dates that auditors and clients commit to work within. It's best to keep an iteration to between two and four weeks, but that choice depends on the fieldwork. After each iteration, the single, combined team pauses to reevaluate and ask:

- » Based on what's been learned, what needs to change?

COMBINING LEAN AND AGILE TECHNIQUES



PRINCIPLES FROM LEAN
- Waste is disrespectful
- Visual management
- Customer defines value
- Standardized work
- Respect for people

PRINCIPLES FROM AGILE
- Iterative development
- Time-boxing
- Value-based prioritization
- Collaboration
- Empirical process control
- Retrospectives

ACTIVE AUDITING PRINCIPLES
- PILLAR ONE – Energetic collaboration
- PILLAR TWO – Iterative audit execution
- PILLAR THREE – Visual management
  - Objectives-based risk assessment
  - Experimentation
  - Retrospectives

- Is the risk assessment still valid?
- Are all the fieldwork steps required to assess the control objective?
- Are the right people involved?
- Where are the bottlenecks?

Both Lean and Agile teach internal auditors to welcome change to their audit program as they learn more and reassess risk. They can't assume initial planning was perfect, so they should embrace an evolving audit. In return, when audits are executed as smaller mini-audits, they become easier to manage because work is done in digestible bites, countermeasures to address problems can be applied in the next iteration, and the audit can be stopped after an iteration and still have useful results.

PILLAR THREE: VISUAL MANAGEMENT

A central principle of Lean is to make waste visible. When waste is visible, the people involved can work together to eliminate it. Frequently, "waste" appears in audit work in the form of waiting, unnecessary motion, rework, and overproduction. Active auditing uses visual management techniques borrowed from Lean to allow the combined team to fully understand the audit's progress and each member of the combined team's part in it.

The greatest waste in auditing involves waiting. Waiting for data to be provided, emails to be returned, interviews to be scheduled, and so on. Internal auditors compensate by shifting their focus to other things, but that means rework as they have to reeducate themselves on the subject when they return to that work. Making lost time visible using visual management tools drives wait time down.

As often as every day for 15-30 minutes, auditors and clients should hold a standup meeting around a visual control board (VCB). The VCB consists of panels that show progress

Agile internal audit is a mindset focused on stakeholder needs, accelerated audit cycles, timely insights, reduced wasted effort, and less documentation, according to Deloitte's 2018 Becoming Agile report.

on the audit program, assigned tasks, a "dog house" for tasks that aren't getting done, a shared master calendar, and a "hearts & minds" board to capture shared expectations and concerns. Because Lean is inherently a change-making methodology, it provides techniques for helping build mutual purpose, and daily standup meetings with the audit clients in front of the VCB are an important example. VCBs can be as large as an entire purpose-built wall or as small as an 11x17 piece of paper taped to a conference room whiteboard. Visual management can ensure:

- Every member of the single, combined audit–client team is constantly updated on status.
- Problems are visible long before they manifest; waiting actions—such as data or report requests—are visible to the entire team, and therefore can be expedited.
- The human aspects of an audit (anxiety, mistrust, etc.) are addressed openly and treated as legitimate risks to the project.

CELEBRATE THE AUDIT

Active auditing borrows two additional important concepts from Agile. The first is retrospectives. In an Agile software project, after each sprint, the team gets together to examine what went well and what should change. This is a critical aspect of improvement and it should occur at the end of every audit, and often at the end of any sizeable iteration. Ceremonies and celebrations are the second concept borrowed from Agile for the conclusion of the audit. The team members come together to celebrate, perhaps with food, and take a moment to reflect on the work they did together.

AUDIT WITHOUT LIMITS

It can be difficult to implement all three pillars at once. The best first step is to start holding frequent, but brief, standup meetings with audit clients and auditors. It will quickly become clear that the standups are more effective with some form of visual management tool. The VCB should be developed early and expanded and refined over time. As standups progress, it should become easier to collaborate more effectively by developing ground rules and acknowledging the human side of the auditor–client relationship.

> **Timely and frequently completed audit work is the outcome of internal auditors and the audit clients working as a single team.**

In the end, the three pillars of active auditing work in concert. Energetic collaboration allows visual management to function smoothly to manage the audit work. Tight monitoring of progress through visual management allows the audit to execute iteratively. Timely and frequently completed audit work is the outcome of internal auditors and the audit clients working as a single team. The specific techniques used are likely to vary among companies and even across audits, but the core concepts contained in each pillar are universal and can be implemented anywhere. Ia

PRESCOTT COLEMAN, CIA, CISA, *is the author of* Active Auditing – A Practical Guide to Lean & Agile Auditing *and the global IT audit director for IHS Markit in Englewood, Colo.*

SANDRA KASAHARA, CIA, CPA, *is a consultant with Umbrella Field LLC in Denver.*

BY MATT KELLY

THE CONTROL–CULTURE CONNECTION

These two elements must complement each other to achieve strong financial reporting.

DEBI ROTH

RAOUL MÉNÈS

All audit committees want strong internal controls over financial reporting, and a strong ethical culture where employees who suspect impropriety feel unafraid to speak about what they see. What is sometimes less understood are the connections between those two things—how corporate culture and internal controls should complement each other, to further the goal of strong, reliable financial reporting. Design them well, and the organization has a powerful buttress against executive misconduct. Don't, and the opposite is just as true.

A fascinating example of this point comes from Bankrate.com, which paid $28.5 million to the U.S. Justice Department earlier this year to settle long-running financial fraud charges. Back in 2011, Bankrate's then-Chief Financial Officer Ed DiMaria concocted a cushion-accounting scheme to manipulate quarterly earnings. He and others fabricated expenses on a bogus spreadsheet, while hiding the true numbers from Bankrate's audit firm. When the U.S. Securities and Exchange Commission (SEC) began inquiring about the company's finances, DiMaria directed others to reply with material not responsive to the SEC's document requests.

Of course this all unraveled eventually. Bankrate announced a restatement in 2014. DiMaria was dismissed, indicted, and sentenced to 10 years in prison. The company hired new outside counsel, and its audit committee cooperated fully with the SEC.

Think about what happened here. First, the company used technology and business processes that gave DiMaria the ability to fabricate financial data while concealing true information. Second, nobody raised alarms about DiMaria's misconduct—not when he lied to the audit firm, not when he misled the audit committee, and not when he had others mislead the SEC.

The issue, really, is about transparency and freedom. Internal audit needs to be able to roam freely through the enterprise to assess risks, and it needs to be able to see real data, rather than whatever report management provides. Or, as Debi Roth, chair of the Audit Advisory Committee for Orange County Public Schools in Florida, puts it: "Can the audit department get it, and pull it themselves?"

That might seem like a straightforward part of governance. In the real world, however, Bankrate is by no means alone. For example, when Polycom Corp. agreed last year to pay $16 million to settle U.S. Foreign Corrupt Practices Act charges, the misconduct was fundamentally similar. Executives in China recorded false information on bogus spreadsheets to hide bribery

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

violations from Polycom's global managers, while masterminding a payoff scheme to Chinese government officials.

Technology and business processes that allow executives to create a false narrative; plus a corporate culture that allows them to *spread* the false narrative—if those are the ingredients for an audit committee's nightmare, what's the antidote? It comes in two parts: strong control activities over financial reporting, and strong corporate culture that encourages everyone to sound the alarms about misconduct.

Ingredient 1: Control Activities

The first ingredient is unimpeded access to the company's transactional data. Access should include not just whatever reports someone might provide to internal audit or the audit committee, but also the actual data about payments, due diligence checks, beneficial ownership, contracts, or whatever else the audit team might want to see.

That's partly a question of technology. Accounting systems should rely on a single data source to make frauds like bogus spreadsheets and false transaction entries harder to accomplish. In an ideal world, auditors should be able to drill down from balance sheet, to line-item accounts, to transactions within those accounts, to supporting documentation for those transactions.

As an audit committee chair, Roth wants to hear the chief audit executive (CAE) explain how the process for gathering data works, and whether there are any concerns about potential interference. For example, does the audit team depend on the IT department to generate reports? That's a risk, no matter how well-intentioned the IT department might be. "I'm looking for the internal audit function to have a good process in place that addresses internal controls, and that they're able to go out and do their job and do it well," she says.

Once upon a time, when companies used data warehouses, the audit team could have access to them, too, and pull whatever information it needed. Today's systems are more complicated, as many firms rely on cloud-based applications that might store data in different locations, or employees might use cloud-based applications but not tell IT about it.

Audit and accounting teams need to think about the design of financial reporting systems and transparency into the data, so that suspicious transactions stick out like a sore thumb.

Ingredient 2: The Control Environment

Even when suspicious transactions are more visible, someone still needs to point them out. After all, at organizations of any appreciable size, many fraudulent activities won't be spotted by the audit team—especially if more than one person is involved in the misconduct, as happened at Bankrate, Polycom, and many others. The organization needs to foster an environment where employees feel comfortable raising concerns about misconduct. "That's always top of mind as an audit committee member," says Raoul Ménès, who serves on the audit committee of the Salt River Pima-Maricopa Indian Community in suburban Phoenix.

"The bad perception to have is, 'Don't worry, internal audit will get it,'" Ménès says. "Well, internal audit cannot see everything. They'll show up for two weeks to do an audit, and then they're gone."

Ménès encourages audit committee members to spend more time at their organizations, getting to know employees casually. Show up early for a committee meeting, for example, and chat with the employees. (That's in addition to any executive sessions at the committee meeting, or any conversations the committee chair has with the CAE between meetings.)

"Meet the audit team, or talk to the controller. Just see how things are going," Ménès says. "When you're able to connect with folks, to work with them and talk with them, they'll open up."

Fair enough, but how else can the audit function identify warning signs about corporate culture? "Auditing culture" is a lofty idea, but a bit vague. Instead, audit teams need to design tests for traits or behaviors that suggest the culture is wrong. Ménès, for example, once worked with a firm where employees received a three-question quiz about the code of conduct shortly after they had certified that they'd read it. The goal wasn't to see how well they memorized the answers; it was to see whether the enterprise had high failure rates as a whole—which would suggest that employees weren't taking the code seriously, a big culture risk.

Roth, meanwhile, wants to hear about managers who try to interfere with auditors' ability to talk to other employees. "If someone is telling the auditor, 'You can't work with anyone else, you have to go through me'—that's an automatic red flag," she says.

Shutting Down Abuse

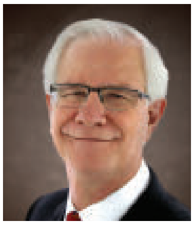
The truth is, an organization can't achieve strong financial reporting without both elements present: systems that provide clear visibility into transactions and a corporate culture that encourages internal audit—or other parts of the enterprise—to put that visibility to good use.

That's the buttress organizations need to thwart executives who might abuse their power to override controls or lie to the board. It can be tough to build in the modern enterprise, with complex IT systems and a globalized workforce. Build it right, however, and that buttress can be pretty powerful. Ia

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

THE IIA's CIA

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



BY J. MICHAEL JACKA

THE CITIZEN INTERNAL AUDITOR

Practitioners should lend their voice, and expertise, to the work of their public sector peers.

Internal auditors working in the public sector experience unique challenges. In many countries, they face a revolving door of elected officials looking toward the next election, appointees glancing over their shoulders to ensure the security of their appointments, and the heightened bureaucracy and red tape inherent with any governmental entity.

But perhaps the most daunting part of the job is that many government audit functions are required to make their final reports publicly accessible. The rest of us can only imagine the challenge of issuing a final report with the entire world watching.

Still, good things can come from potentially negative situations. One government audit function, for example, leveraged the reporting requirement by establishing its own website and using it to showcase the results of its work. The site showed internal audit's positive contributions, providing constituents with concrete evidence of how tax dollars spent on auditing helped everyone. Imagine the opportunity to speak directly to stakeholders, explicitly showing the value auditing provides.

Practitioners may want to consider another upside to the public nature of this process—depending on where you reside, audit reports related to the various communities, municipalities, and governments associated with your area may be available for your perusal. At any time, you can go to the internet and find what is happening in your city, county, state, or other governmental entity.

Where civic participation is an option, internal auditors have two duties to uphold as citizens. The first mirrors that of any citizen—to become engaged in local government and the activities of public officials. But internal auditors also have something most other citizens lack—the professional knowledge and experience required to understand public sector audit work. We are uniquely equipped to understand how local government uses the audit function, as well as the broader impacts on governance, risk, and assurance.

The challenge is to take the time to explore various local government websites and find those audit reports. Auditors can then determine if it looks like the audit function is examining the important areas, if their findings are important, and whether those responsible are addressing the findings. They can also determine if elected officials are taking the reports, results, and issues seriously.

If government entities fall short, internal auditors should step forward—as both citizens and professional internal auditors—and make their voices heard. Write letters and emails, speak up at open meetings, request a private meeting, and make elected officials understand the importance of internal auditing. If your voice is ignored, reach out to fellow professionals to help elected officials understand who they work for. Because when they work for internal audit professionals, those officials have an increased duty to ensure a strong governance structure—and a strong audit function—is helping everyone succeed. Ia

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

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

A CHANGE IN MINDSET

Getting up to speed with data analytics is neither a resource nor a skills issue.

KEN PETERSEN
Product Manager
Wolters Kluwer
TeamMate

DAN ZITTING
Chief Customer
Experience Officer
Galvanize

How far have audit functions come in terms of data analytics usage?

PETERSEN Progressing audit analytics is a journey that doesn't have an end, but I'm excited to hear organizations describe how they continue to progress year over year. These organizations know the direction they need to go, continue to raise the bar for themselves, and set new objectives to achieve. They face the same resource limitations many audit teams do, so they encourage all their auditors to progress, not just those assigned as the data analytics expert.

ZITTING Not far enough. Recently, my company's State of the GRC Profession survey revealed 43% of professionals want to grow their data analysis skills, but those figures have been the same for years—if not decades. Leading audit teams that are willing to embrace change and take risks are indeed creating a new future by delivering and sharing successes in data analysis, advanced analytics, robotic process automation, and even machine learning/artificial intelligence; unfortunately, these leaders are the exception. They inspire us, yet other corporate functions like marketing, IT/digital transformation, security, and even risk management are leaving internal audit behind.

What are examples, beyond typical usages, of analytics that auditors should be undertaking?

ZITTING Let's not write off the "typical usages" of data analytics, because the vast majority of audit teams aren't even doing those. The key control areas that virtually every organization's audit and internal control teams test are completely automatable, yet few seem to do it. Areas like user access, IT administrator activity (or other activity log testing), journal entry, payment, and payroll should never again be tested with anything but data analytics.

Beyond that, the universe of possibility for the data-savvy audit team is limitless. I'm seeing leading audit teams even turn analytics in on themselves—like doing textual analytics on the text of the past several years' audit findings to indicate where risk is increasing or not being addressed. It's incredibly impactful. I've also seen practitioners develop analytics that use machine learning to create "hot clusters" of employees that are at high risk of churn, or to see "hot clusters" of payments that could be bribes, money laundering, or sanction violations.

PETERSEN How about running data analysis on the audit analytics program? Start by ascertaining how many audits contain some level of data analysis—sampling doesn't count. Now compare that to how many should contain some analysis. I don't know of any organizations that would find they should be doing analytics on 100% of their audits, but if they are

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

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

honest, they'll find a significant gap between those audits that could have some analytics performed and those that do.

Now that we have determined breadth of coverage, let's determine depth of coverage. This is done by determining for each of those audits that could have analytics performed on them, the analytics that would ideally be performed. Internal audit should focus on those analytics it would be proud to report to the audit committee that it performed considering the risks and audit objective. Don't be discouraged by the thought that internal audit can never achieve the coverage it has identified. Instead, plan to increase coverage each year.

How can small audit functions that can't afford a data scientist jump into data analytics?

PETERSEN Start with basic analytics functions. Audit leadership needs to lead the organization to continually progress the analytics being performed. Leverage those individuals in your organization that have an aptitude for analytics and communicate within the team successes, new ideas, and new ways of doing things. Use known tools such as Excel and easy-to-use and learn audit analytics tools. Leverage existing audit techniques across different types of audits. For example, testing for duplicate payments, separation of duties violations, and several other routines apply across many types of audits. Once you've determined how to identify these in one audit, this can be applied to other audits. Teams without a data scientist can still have a strong audit analytics program.

ZITTING Every audit function that can hire a single auditor can afford a person with data skills. The problem is that we accept the status quo of the short-term demands of internal audit's stakeholders; thus, we elect to hire a "traditional" auditor over a person with technical data skills and the ability to think critically. Obviously, that is a necessity in real life, but also it illustrates that the "can't afford" or "can't find the skills" arguments are basically bad excuses that abdicate our responsibility as corporate leaders to evolve with the economic demands of the modern environment. Consider a complete shift in mindset. What if we were building a small data science team that had some audit skills instead of a small audit team with some data skills? Wouldn't that change our perspective on staffing for a truly modern form of auditing?

What skills should audit functions be looking for when hiring a data analytics expert?

ZITTING Most importantly, audit functions should be looking for critical thinking skills. Technical skills in data analytics can be taught. What is difficult to teach is critical thinking, particularly as it relates to knowledge of audit process/risk assessment/internal control, knowledge of the business and its strategy/operations, and the ability to navigate corporate access challenges—access to data and executive time—by asking really smart questions. Next, look for an understanding and desire to work in an Agile mindset. Specific tools and approaches will always change, but if the candidate understands Agile methodology—minimum viable product, sprints and iteration, continuous improvement—he or she will be able to deliver business results in both the short and long term regardless of issues of tool preference.

PETERSEN Communication and collaboration skills can exponentially increase the team's analytics effectiveness. Without these skills, there is one expert off doing analytics by him or herself. However, with these skills and easy-to-use analytics tools, the expert can guide the entire team through its analytics needs, greatly increasing the overall effectiveness of the team. When not providing this guidance, the expert can work on more complex analytical projects. This approach also increases employee satisfaction of both the expert and the other team members.

What does a best-in-class audit function that is fully embedded in data analytics look like?

PETERSEN These teams apply a quantitative analysis and measurement to their audit analytics. They do this by measuring the depth and breadth of their analytics coverage. They have strong leaders who promote the value of analytics and make it a part of the team's culture. They also understand that there is no finish line, but the analytics program will continually evolve and grow. Leaders of these teams incorporate all team members into the analytics process, understanding that some have a stronger aptitude for it than others, but still expecting all to participate, and they set appropriate analytics goals for each. Not only are organizations like this best-in-class with respect to the analytics functions but, as a surprise to some, they also have happier team members.

ZITTING The best audit organizations already are demonstrating that their core skill is data analysis. It's the only way to get large-scale insight on risk, control, and assurance across globally dispersed organizations using constrained resources. Best-in-class audit functions don't embed data analytics, they provide 90% of all assurance they report through analytics and reserve "traditional" auditing for manual deep dives into areas of significant risk or deviation from policy, regulation, or other standards of control. For example, one of our clients moved its entire internal audit team into the core business operation and began rebuilding internal audit from scratch in the last two years. This was because audit was providing so much value via its complete focus on data and analytics, the business demanded to consume the function, and the audit committee agreed to rebuild. That's one example of internal audit driving real value through a data-centric mindset and practice. Ia

IIA Calendar

IIA CONFERENCES

www.theiia.org/conferences

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

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

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

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

SEPT. 20–22
Internal Audit Student Exchange
Rosen Centre Hotel
Orlando, FL

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

IIA TRAINING

www.theiia.org/training

SEPT. 9–12
Vision University
San Diego

SEPT. 9–18
Root Cause Analysis for Internal Auditors
Online

SEPT. 9–20
CIA Exam Preparation – Part 1: Essentials of Internal Auditing
Online

SEPT. 10
Fundamentals of Internal Auditing
Online

SEPT. 10–13
Multiple Courses
New York

SEPT. 10–18
CIA Exam Preparation – Parts 1, 2, & 3
Lake Mary, FL

SEPT. 17–20
Multiple Courses
Boston

SEPT. 17–20
Tools & Techniques III: Audit Manager
Philadelphia

SEPT. 17–26
Cybersecurity Auditing in an Unsecure World
Online

SEPT. 23–OCT. 2
The Effective Auditor: Understanding and Applying Emotional Intelligence
Online

SEPT. 24–27
Multiple Courses
Dallas

SEPT. 24–OCT. 3
Fundamentals of IT Auditing
Online

SEPT. 30–OCT. 11
CIA Exam Preparation – Part 3: Business Knowledge for Internal Auditing
Online

OCT. 1–4
Multiple Courses
Chicago

OCT. 8–11
Tools & Techniques II: Lead Auditor
Charlotte, NC

OCT. 8–17
Building a Sustainable Quality Program
Online

OCT. 15–17
COSO Internal Control Certificate
New York

OCT. 15–17
IT General Controls
Online

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

PHOTO: RAWPIXEL.COM / SHUTTERSTOCK.COM

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

BY PERRY MOORE

A LESSON IN ETHICS

The importance of professional integrity needs to be learned early in one's audit career.

Recent reports of the extremes some parents have pursued to get their children admitted into elite colleges have raised questions about what example these parents are setting for their children. In some cases the children were unaware of their parents' extraordinary efforts, though others allegedly knew about it and therefore may have been complicit. Perhaps the scandal comes as no surprise to many in the audit profession—after all, we see cheating, rule bending, and outright falsehoods regularly. But rather than simply shrugging our shoulders and pretending it has nothing to do with us, internal auditors need to be part of the solution.

Research suggests that dishonesty among students is common. Donald McCabe, founding president of the International Center for Academic Integrity, analyzed surveys of nearly 71,000 college students conducted between 2002 and 2015. He reported that 39% admitted to cheating on tests, and 68% admitted to some form of cheating. Why do college students cheat? They want a good job and career.

Think about that last statement—college students cheat to get a job. Many of them obtain their first job as new hires in the audit department. If these students view cheating as acceptable, what can internal auditors do to help them understand their organization's ethical expectations, as well as those of the internal audit profession?

Many years ago, a university colleague shared with me the story of a phone call he received from a local employer. The firm's representative bluntly asked what the university was teaching its students, as his company had just caught an auditor signing off on an audit program for work not actually performed. My colleague privately observed later that he had always thought this individual, as a student at our university, had cheated in his classes, even though he never caught him in the act. From a professional viewpoint this anecdote points to a big risk—students who cheated in college may continue to cheat in their career.

Efforts to address such risk should begin as soon as students enter the workforce. Internal audit onboarding activities and employee mentoring, for example, should be aimed at helping new hires do the right thing. Encouragement should focus on guidance to help them comprehend what it means to be an internal audit professional—including adherence to ethical standards. Recent graduates should be reminded that behavior they may have viewed as acceptable in college is not acceptable in the workforce.

We also need to promote success stories of individuals who have not cheated—of those who exemplify high standards of ethical conduct. We should celebrate individuals who stopped a fraud from happening, or who helped prevent the company from erring in judgment. Sending the right message up front will help the next generation of audit practitioners make good choices and maintain the standards of integrity that have long defined our profession. Ia

PERRY MOORE, PHD, CIA, CRMA, *is Charles E. Frasier Professor of Accountancy, Pfeffer Graduate School of Business, Lipscomb University, in Nashville, Tenn.*

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