Ia
INTERNAL AUDITOR

OCTOBER 2019 A PUBLICATION OF THE IIA

EMERGING LEADERS 2019

These professionals are eager to expand internal audit's influence into new areas of collaboration with leadership.

Wolters Kluwer

TeamMate

Leading Audit Evolution

New OnDemand Demos

TeamMate+ Audit

Get a comprehensive look at the latest version of TeamMate+ Audit, its most powerful benefits, and see how TeamMate is leading audit evolution.

TeamMate+ for Combined Assurance

Experience TeamMate+ first hand and see how it drives the critical coordination between your lines of defense.

TeamMate+ for Strategic Audit Planning

Watch how TeamMate+ can help elevate the audit function and its value to key stakeholders.

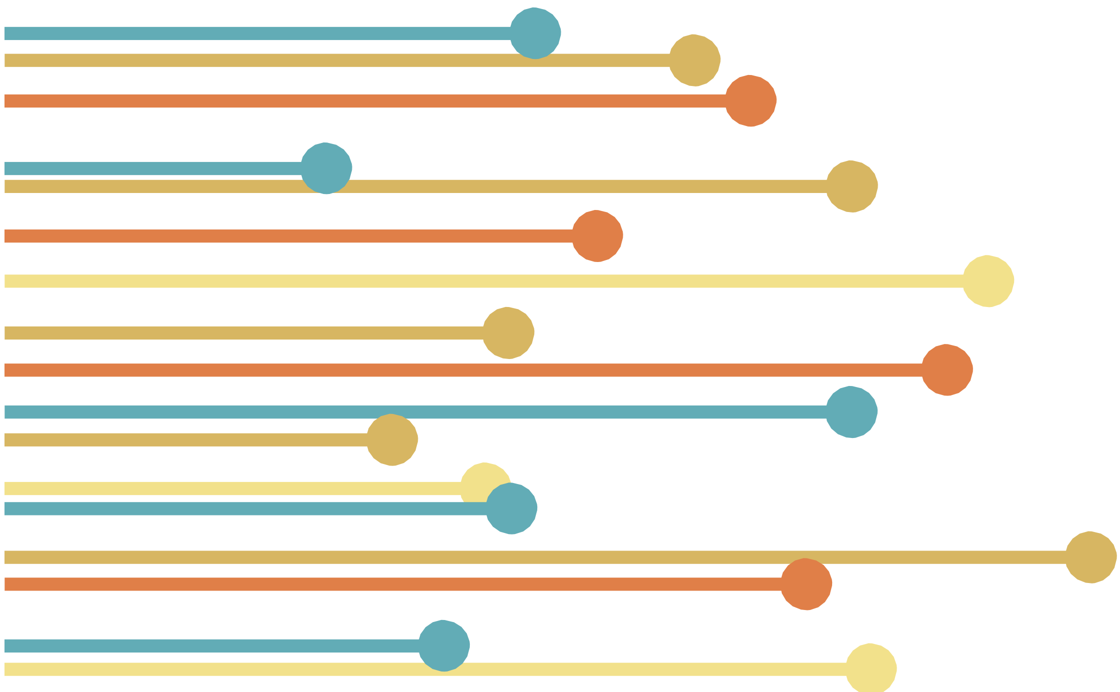
and more…

View a Demo today at **TeamMateSolutions.com/Demo**


"My CIA proves I am committed to providing value to my organization."
Emiko Tai, CIA, CCSA
Japan
CIA Since 2003
CIA Proves Credibility and Proficiency.
Get started today at www.theiia.org/CIA.

Ia
INTERNAL AUDITOR

OCTOBER 2019 VOLUME LXXVI: V



FEATURES


How do you turn trust to your competitive advantage?
EY
Building a better working world
The better the question. The better the answer.
The better the world works.
© 2019 EYGM Limited. All Rights Reserved. ED None.

Ia

INTERNAL AUDITOR

OCTOBER 2019 VOLUME LXXVI: V

DEPARTMENTS

ONLINE InternalAuditor.org

Auditing With Grit Persistence, courage, and character are key differentiators for achieving success. Do you have what it takes to be a gritty internal auditor?

Emerging With Insight In our latest video series, some of this year's Emerging Leaders share important lessons from their careers and offer advice for those just entering the audit profession.

The Business of Ethical AI Research finds that most employers aren't concerned about artificial intelligence (AI) ethics and haven't created policies for ethical use of AI.

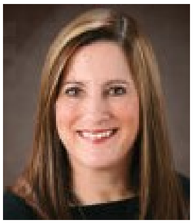
Protecting the Protectors Military personnel are a prime target for identity thieves, so military organizations need to restrict access to service members' personal information.

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, USA. 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, USA. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001.

TOP: ANASTASIIA_NEW / ISTOCKPHOTO.COM, BOTTOM: JULIAN WISKEMANN / SHUTTERSTOCK.COM

Editor's Note



INTERNAL AUDIT'S EMERGING STARS

This marks the seventh year *Internal Auditor* has recognized emerging leaders in the internal audit profession. Our 2019 Emerging Leaders (see page 22) join 100 other young professionals who have been recognized since 2013.

Past honorees have not rested on their laurels, but instead, as expected, continue to achieve great things. For example:

- » At the time they were named Emerging Leaders, 74 had their Certified Internal Auditor (CIA) designation. Today, 89 are CIAs.
- » Since being named an Emerging Leader, 71 have new job titles or have moved to new companies.
- » Three Emerging Leaders have served on The IIA's North American Board and Global Board of Directors. Seventeen leaders have served on one or more of The IIA's committees.
- » Emerging Leaders have written 88 blog posts/articles for the magazine, and 46 leaders have been interviewed for *Internal Auditor* articles.

Two former Emerging Leaders, Leslie Bordelon (2014) and Alex Rusate (2017) share how their careers have progressed since their recognition in this issue's "Eye on Business" (see page 60). Rusate, for example, has obtained three new certifications since 2017. Bordelon and Rusate offer up-and-coming internal auditors advice on how to advance in the profession and explain why they stay in internal auditing. Bordelon says she's excited about the future of the profession. "As companies start to embrace new technologies such as machine learning and robotic process automation, internal audit teams have to really rethink how they approach their work," she says.

Technology is a theme throughout the "Emerging Leaders 2019" article. "In fact, emphasizing analytics seems almost old-fashioned to the 2019 honorees; they assume analytics are key to internal audit and continually expand their skills—often on their own time," writes author Russell Jackson. This year's leaders recognize that this expertise can open doors for internal auditors, and they're eager to be meaningful players in their organization's success, Jackson says.

On another note, when you're Wright, you're Wright. With this issue, we wish "Risk Watch" contributing editor Charlie Wright a fond farewell and introduce Rick Wright (no relation) as the new contributing editor. A big thank you to Charlie for his time and effort, and for the outstanding contributions he's made to this department. We are fortunate to have Rick as Charlie's replacement beginning in December. Rick is the director of internal audit and enterprise risk management for YRC Worldwide. He is also the author of *The Internal Auditor's Guide to Risk Assessment* and *Internal Auditing: Uncover the Myths, Discover the Value.* Welcome, Rick!

Anne

@AMillage on Twitter

Reader Forum

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

Getting Up to Speed

Thank you for your great "Back to Basics" department. I have nearly a decade of public accounting audit experience but stepped into the internal audit world just over a year ago. While there is a lot of overlap between internal and external auditing, there is still a lot to learn. The department, especially August 2019's "Expand Your Role in Internal Audit," is a great resource to get me up to speed.

STEVE LOFLIN *comments on Alex Rusate's "Expand Your Role in Internal Audit" ("Back to Basics," August 2019).*

Measuring Culture

I agree culture is really important, and it's good to contribute, but I'm concerned where you are taking this for internal auditors who are new to this area. It would be easy to do work here and be detached from The IIA's *International Standards for the Professional Practice of Internal Auditing*. What is the key risk concerning culture/behavior that you are looking at? Who is managing the risk of problems in lines one and two and with what metrics? By what criteria is internal audit going to judge management's approach? What insight is internal audit planning to give?

I continue to fear false assurance by internal audit teams in this area by thinking culture is a thing that can be measured and managed and, quite possibly, missing a subculture problem or a behavioral/political problem concerning a key risk (especially beyond compliance).

J. PATERSON *comments on Jim Roth's online series, "Auditing Culture: Observation and Data" (InternalAuditor.org).*

Author's Response: *I don't disagree with anything you say. In my own training programs, I emphasize that the objective of culture auditing is not to reach a firm conclusion about the overall culture or the subculture of an area. It is to continually enrich stakeholders' understanding of the culture through a combination of qualitative and quantitative evidence. No single tool, technique, or approach should be relied on, and we must be careful not to give false assurance. Nor should internal audit see itself as the sole provider of cultural assurance.*

What I am trying to do in this series of articles is give readers a variety of approaches in enough concrete detail that they can consider what may or may not work in their own organizations. It goes without saying that we must be risk-based, conform to all our Standards, *and tailor what we do to our own organizations.*

MORE

VISIT InternalAuditor.org for the latest blogs

Ia INTERNAL AUDITOR
OCTOBER 2019
VOLUME LXXVI:V

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

EDITORIAL ADVISORY BOARD
Jennifer Bernard Allen, cia Dennis Applegate, cia, cpa, cma, cfe Lal Balkaran, cia, fcpa, fcga, fcma
Andrew Bowman, cpa, cfe, cisa
Mark Brinkley, cia, cfsa, crma
Robin Altia Brown
Adil Buhariwalla, cia, crma, cfe, fca
Wade Cassels, cia, ccsa, crma, cfe
Stefanie Chambers
Faizal Chaudhury, cpa, cgma
Michael Cox, fiia(nz), at
Haylee Deniston, cpa
Kayla Flanders, cia, crma
James Fox, cia, cfe
James Gager
Michael Garvey, cia
Jorge Gonzalez, cia, cisa
Nancy Haig, cia, cfe, ccsa, crma
Sonja Heath, cia
Kyle Hebert, cia
Daniel Helming, cia, cpa
Karin L. Hill, cia, cgap, crma
J. Michael Jacka, cia, cpcu, cfe, cpa
Sandra Kasahara, cia, cpa Michael Levy, cia, crma, cisa, cissp Merek Lipson, cia
Thomas Luccock, cia, cpa
Michael Marinaccio, cia
Alyssa G. Martin, cpa
Joe Martins, cia, crma
Dennis McGuffie, cpa
Stephen Minder, cia
Rick Neisser, cia, cisa, clu, cpcu
Hans Nieuwlands, cia, ra, ccsa, cgap
Manish Pathak, ca
Bryant Richards, cia, crma
Jeffrey Ridley, cia, fcis, fiia
James Roth, phd, cia, ccsa
Katherine Shamai, cia, ca, cfe, crma
Debora Shelton, cia, crma
Laura Soileau, cia, crma
Jerry Strawser, phd, cpa
Glenn Sumners, phd, cia, cpa, crma
Robert Taft, cia, ccsa, crma
Brandon Tanous, cia, cgap, crma
Stephen Tiley, cia
Robert Venczel, cia, crma, cisa
David Weiss, cia
Scott White, cia, cfsa, crma
Rick Wright, cia
Rodney Wright, cia, cpa, cfsa
Benito Ybarra, cia

IIA PRESIDENT AND CEO
Richard F. Chambers, cia, qial, cgap, ccsa, crma

IIA CHAIRMAN OF THE BOARD
J. Michael Joyce, Jr., cia, cpa, crma

PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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

LYNDON Group

Audit Your Spend

When was the last time your organization audited travel, entertainment and other business expenses?

Lyndon Group's audit services focus on:

OPERATIONS

- Efficiency
- Savings
- Usability

REPORTING

- Allocations
- Analytics
- Reconciliations

COMPLIANCE

- Contracts
- Policies
- Regulatory

Visit us at www.lyndon-group.com/auditservices

Follow us @Lyndon-Group

SAP® Concur® Partner Solution Provider

SAP® Concur® Partner Customer Success

Hackers outpacing security defenses... Assessing third parties continually... Internal audit becoming cybersecurity ally... NIST releases AI standards plan.

Update

MODERN DATA HURDLES

A variety of obstacles have kept nearly two-thirds of businesses from fully implementing data modernization.

55%	Budget/cost
44%	Lack of understanding of technology
41%	Lack of consensus among decision-makers
40%	Lack of clarity on metrics

Source: Deloitte, Data Modernization and the Cloud: Which Trend Is Driving the Other?

THE PURPOSE OF BUSINESS

Companies should focus on stakeholders and values, Business Roundtable says.

The purpose of a company is to serve stakeholders—not just earn money for shareholders—according to a statement from the Business Roundtable. The revised Statement on the Purpose of a Corporation was signed by 181 CEOs of the largest companies and reverses the Washington, D.C.-based business lobbying group's long-standing position.

"Businesses play a vital role in the economy by creating jobs, fostering innovation, and providing essential goods and services," the statement notes. The co-signing CEOs commit to delivering value to customers, investing in employees, dealing fairly and ethically with suppliers, supporting their communities, and generating long-term value for shareholders. "These modernized principles reflect the business community's unwavering commitment to continue to push for an economy that serves all Americans," says Jamie Dimon, chairman and CEO of JPMorgan Chase & Co. and chairman of the Business Roundtable.

The Business Roundtable's change of position is being met with skepticism, though, with some critics decrying the shift away from a traditional shareholder-centric purpose. Others note the statement doesn't reflect today's purpose-driven workforce.

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

IMAGES: TOP, ANASTASIIA_NEW / ISTOCKPHOTO.COM; LEFT, DOOMU / SHUTTERSTOCK.COM

"These five things, you're supposed to be doing now," said Gallup Chairman and CEO Jim Clifton in a Gallup podcast.

Harold Silverman, IIA managing director of CAE Services, said the Business Roundtable statement is an opportunity for internal audit to provide assurance that the organization's actions are consistent with its stated values. During a CAE Podcast from The IIA's Audit Executive Center, Silverman advised looking at these values by reviewing internal controls. "It sets an expectation that organizationally, the truth matters in all types of external reporting," he said. —T. MCCOLLUM

SECURITY LEADERS ANTICIPATE MORE ATTACKS

CISOs foresee increased hacking, cite preparedness concerns.

More than 80% of chief information security officers (CISOs) say they expect the risk of cyberattacks to increase, according to a global survey of more than 200 CISOs by Forbes Insight and cybersecurity firm Fortinet. The Making Tough Choices research also shows that nearly one-fourth of respondents say attackers' capabilities are outpacing their ability to defend the organization.

In their efforts to stave off breaches, security leaders say they are allocating, on average, more than one-third of their security budget to response. But ideally, the CISOs point out, they would like to see that percentage increase. Moreover, they cite talent and training constraints as a significant impediment to security efforts, prompting CISOs to pay increased attention to educating their own employees and building cybersecurity awareness organizationwide.

Safeguarding customer data represents a top priority for survey respondents, with 36% citing it as their main security focus, followed by protecting the organization's brand. Most respondents also say protecting intellectual property is an area of focus. —D. SALIERNO

82% OF CFOS SAY THEY COLLABORATE WITH THEIR COMPANY'S CIO MORE NOW THAN THREE YEARS AGO.

56% OF CFOS AND CIOS ARE COLLABORATING ON TECHNOLOGY INVESTMENTS, and 52% are working together on business system changes.

"Providing opportunities for the [finance and IT] teams to collaborate builds awareness of operational challenges and needs, which often leads to more astute insights on best practices and solutions," says John Reed, an executive vice president for Robert Half.

Source: Robert Half, Survey of 1,000 U.S.-company CFOs.

ITERATION IS THE NEW IMPERATIVE

Rapid change necessitates continual third-party assessments.

The standard point-in-time approach to risk management is no longer effective in today's fast-paced, rapidly changing business landscape, a report from research and advisory firm Gartner Inc. asserts. With an increasing number of third parties performing new and different types of services, the research says, organizations can't always identify material risks before starting a business relationship.

The report, Stay Ahead of Growing Third-party Risk, surveyed more than 250 legal and compliance leaders in the U.S. Among respondents whose organizations engage third parties for business services, 83% say

IMAGES: TOP, BSWEI/ SHUTTERSTOCK.COM; RIGHT, FOTOGESTOEBER/ SHUTTERSTOCK.COM

MORE VISIT InternalAuditor.org to read an extended interview with DaMon Ross Sr.

they identified third-party risks after conducting due diligence and before recertification. Moreover, 31% of those risks had a material impact on the business.

Modern risk management, the report states, must account for ongoing changes in third-party relationships and mitigate risks in an iterative way — that is, continually, rather than at specified intervals. "Our research shows an iterative approach to third-party risk management is the new imperative for meeting business demands for speed and stakeholder demands for risk mitigation," says Chris Audet, research director for Gartner's Legal & Compliance practice.

The report cites several factors to help explain the changing nature of third-party risk and its increased importance as an area of organizational focus. For example, 80% of respondents use third parties, including startups and business model innovators, rather than incumbent service providers, to provide new-in-kind technology services at their organizations. Two-thirds say third parties are providing services outside of the company's core business model. Gartner also notes third parties now have greater access to organizational data, and they are working with an increasing number of their own providers — spawning fourth and fifth parties.

—D. SALIERNO

CYBERSECURITY'S KEY ALLY

Internal audit should be a strong cybersecurity advocate, says DaMon Ross Sr., senior vice president and head of Cybersecurity Operations for SunTrust.

What is the relationship between IT and internal audit in cybersecurity and preparedness? IT is essentially the assets that cybersecurity is supposed to be protecting. Internal audit should ensure technical and nontechnical controls are in place and operating effectively. Internal audit personnel must become intimately familiar with cybersecurity and how to test the effectiveness of cyber controls. Too often, internal auditors are not technical enough to assess whether an organization's cyber controls are adequate to protect the assets they were put in place to protect.

Internal audit's most valuable role is ensuring cybersecurity functions have the resources necessary to protect the organization effectively. Whether those resources be funding, staffing, or data from the organization's IT systems, internal audit should be a strong advocate for the cybersecurity function by raising awareness around the organization's cybersecurity needs. Internal audit assessment results should be a major topic in C-suite briefings to ensure the cybersecurity function receives the support necessary to protect the organization.

UNCHARTED AI

U.S. NIST has a plan for developing artificial intelligence standards.

Artificial intelligence (AI) standards need to be flexible enough to stimulate innovation and adapt to new technologies, according to a U.S. National Institute of Standards and Technology (NIST) plan. Such standards also must minimize bias and protect privacy, notes the U.S. Leadership in AI document.

"This plan provides a path to ensure the federal government supports AI standards that are flexible and inclusive," says Walter Copan, undersecretary of commerce for Standards and Technology and NIST director.

Along those lines, the plan identifies nine focus areas: concepts and terminology, data and knowledge, human interactions, metrics, networking, performance testing and reporting methodology, safety, risk management, and trustworthiness.

It also calls for the U.S. government to bolster AI standards-related knowledge, leadership, and coordination among federal agencies and promotes research that explores how trustworthiness can be added to standards and standards-related tools. Moreover, the plan advocates developing AI standards through expanded public-private partnerships. **—S. STEFFEE**

PHOTO: LEFT, VS148 / SHUTTERSTOCK.COM

Back to Basics

BY CHRISTINE HOGAN HAYES EDITED BY JAMES ROTH + WADE CASSELS

COMMUNICATION SKILLS FOR SUCCESS

Newly promoted senior auditors need to master the skills that help develop less experienced auditors.

After gaining years of internal audit experience, associate internal auditors may be promoted to senior internal auditor. Internal audit management may recognize the auditor's professional growth and want to encourage continued development.

Senior internal auditors are responsible for leading audits across the organization while working with associate internal auditors on various audit projects. Through many years' experience, senior auditors have had extensive opportunities to hone internal audit-specific skills, such as testing, workpaper execution, and audit report writing.

New senior auditors may not have experience in the area of developing and coaching the individuals on their audit project team. And while senior auditors may have strategies for teaching internal audit practices and processes, they might not possess the skills that help develop a well-rounded associate auditor. Therefore, it is the senior auditor's responsibility to not only understand what promotes the professional growth of associate auditors, but also the strategies for effectively teaching the skills that ensure success. How the skills are taught often impacts the ability to grasp new internal audit concepts and processes.

Three key communication skills for new senior auditors to master are language selection and usage that encourages learning and growth, demonstrating strong communication skills to strengthen the skills of the team, and facilitating strategic communications through business partnerships. These skills cover the various interactions internal auditors experience daily.

1. Language Selection

A senior auditor's word selection, tone, and inflection can make a tremendous difference in the effectiveness of communication. One area in particular is providing constructive feedback. Such feedback, while both well-intentioned and important, may not be well-received because of the inflection and tone of voice. Some associates may be able to hear the message through the inflection and tone, but others may focus solely on it, and completely miss the objective of the message.

To assess the associate auditor's understanding when explaining an internal audit concept, the senior auditor might ask, "Does that make sense?" versus "Are we okay?" or "Are we good?" This makes a difference in determining progress and encouraging discussion. While it may be well-meaning, "Does that make sense?" is phrased in such a way that might not permit feedback (and if it does, is focused on the topic being taught). "Are we

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

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

okay?" can open dialogue for the associate auditor to ask questions, as well as voice concerns. Using "we" indicates that the learning process involves both the internal audit senior and associate. This phrasing can sometimes encourage a broader conversation, rather than solely confirming a successful transfer of knowledge.

Simple changes in wording can have a huge impact on the team's morale and skill development, especially because associate auditors may have varying professional backgrounds and different learning styles. Word choice, tone, and inflection can help reinforce the meaning of one's mes- sage and encourages professional and productive discussions.

2. Demonstrating Communication Skills

When a senior auditor thoughtfully considers language, and makes necessary changes in phrasing and tone to best support the team, it is appropriate to then demonstrate his or her communication skills. As senior auditors work with a variety of stakeholders, they should consider their written and oral communications.

Written Communication New associate auditors who are learning the internal audit department culture will undoubtedly copy the communication style of their leaders; therefore, it is critical to reflect upon one's own written communication and replace bad communication habits with a strong communication style. After all, one cannot hold associate auditors to a high communication standard if senior auditors are not modeling appropriate communication skills, themselves. From time to time, jargon is used in memorandums and emails are sent lacking punctuation, grammar, or spelling. Associate auditors are included in correspondence, so professional language and communication should be used in all interactions. Even if it takes a few extra minutes, senior auditors should proofread written communication.

> Careful planning is necessary to set up the individual and team for success.

Oral Communication Exposing associates to various learning experiences is important; however, careful planning by the senior auditor is necessary to set up the individual and team for success. For example, if an associate auditor has never presented in front of audit client management, why have him or her present for the first time at the closing meeting, which may be more sensitive than the opening meeting? The associate may be successful, but chances are, without experience, he or she will flounder. Such unplanned approaches to training decrease team morale, and send a message to the audit client that internal audit is not a supportive and growth-focused department. A planned and intentional approach to communication training sends a message that the senior auditor cares not only about the success of the audit, but the associates, too.

3. Strategic Communication

Strong business partnering relationships are often built in informal ways, whether that be a walk around the office during lunch, a short coffee break, or by dropping by someone's office. Chances are that at one time or another, a leader within the internal audit department has included the recently promoted senior auditor in such opportunities. By including associates in such interactions, it helps them build their own network and demonstrates the way in which to build their own relationships with leaders throughout the enterprise. This can help improve the image and reputation of the internal audit department within the organization.

Senior auditors also can help facilitate opportunities for communication skill improvement among associate auditors through the presentation of technical skills. Associate auditors may have professional and educational backgrounds in areas outside of the department under review, but possess specialized skills in subjects such as predictive modeling and project management. These skills are not only valuable in their application within the internal audit role, but they are also useful across the enterprise. When appropriate, senior auditors can initiate the conversation among business management about the possibility of a workshop or webinar, for example, and encourage the associate auditor to share his or her expertise with audit clients.

Fostering Success

Being promoted from associate internal auditor to senior internal auditor is reason to celebrate one's professional accomplishments. However, with such promotion comes increased responsibility. And to foster further success, it is necessary to implement the communication skills that will progress one's own professional development, as well as help improve the skills of emerging talent within the internal audit department.

CHRISTINE HOGAN HAYES *is an internal audit supervisor at Plymouth Rock Management Co. of New Jersey in Woodbridge.*

BY SEYYED MOHSEN HASHEMI EDITED BY STEVE MAR

TOP CHALLENGES OF AUTOMATING AUDIT

Internal audit must transform its own processes to keep pace with the business transformation occurring in the organization.

Organizations are rapidly adopting technologies such as cloud computing, robotic process automation (RPA), machine learning, blockchain, and cognitive computing to create tomorrow's business in today's market. Internal audit needs to transform its processes to keep pace with these changes, and IT audit processes are an excellent place to start this transformation.

Organizations that still perform most internal audit tasks manually complicate IT governance. In this manual model, auditors have adopted many compliance laws, policies, procedures, guidelines, and standards, along with their related control objectives. Moreover, internal audit manages audit process elements such as training, standards, risk, planning, documentation, interviews, and findings separately.

An automated internal audit process can enable the audit function to link, consolidate, and integrate the planning, performance, and response steps of the audit process into a holistic approach. The process should present audit recommendations in a way that is dynamically sustainable within the organization's integrated action plans.

Since 2012, many standards and frameworks have changed their models, procedures, and guidelines to elaborate on the role of the IT governance process. Accordingly, internal audit should redesign its processes to coincide with new, streamlined IT processes and related roles. Meanwhile, IT audit specialists should understand the interoperability among the conceptual models of IT management, governance, standards, events, audits, and planning.

Transforming audit processes comes with challenges, though. Each of these challenges can be encapsulated in a pattern of a problem and a solution, which internal audit can prioritize based on its stakeholders' needs.

1. Syncing the IT Audit Process With IT Project Planning

Problem: IT audit teams need a way to link, tailor, and update audit findings and recommendations for ongoing IT projects and action plans. This will be necessary for auditors to follow up on findings and identify who is responsible for carrying out audit recommendations.

Solution: An automated IT audit system would break IT audit work into two levels—findings' recom- mendations and their final conditions — encompassing all preventive, detective, and corrective controls. The recommended actions reported in audit findings should be linked, integrated, and synced by their related IT project's nondisclosure agreements, service-level agreements, and contracts. Then, the automated IT

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

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

audit system should confirm that management addressed the recommendation.

2. Letting IT Governance Direct the IT Audit Process

Problem: The role of the IT audit team in corporate governance is important because the function can help bridge the gap between the business and IT in organizations. IT governance is a key part of corporate governance, which directs and monitors the finance, quality, operations, and IT functions. Three of these functions — finance, qual- ity, and operations — are being transformed by innovative, technology-based processes. Thus, the problems are how the board and executives will design and implement a corporate governance system and how the IT governance process will be automated.

Solution: Automating the IT governance process should be comprehensive and agile. In other words, the IT governance, risk, and control mapping and cascading of goals and indicators among all levels of the organization must be user-friendly. To have an agile audit function, though, these maps and cascades should be tailored based on the types of governance roles such as the board, executives, internal auditors, chief information officer, and IT manager.

The internal audit function also should map key performance indicators based on the control objectives of various regulations, standards, and frameworks into its goals. These governance requirements include frameworks from The Committee of Sponsoring Organizations of the Treadway Commission and the U.S. National Institute of Standards and Technology (NIST), industry requirements such as the Payment Card Industry Data Security Standard, and regulations such as the European Union's General Data Protection Regulation and the U.S. Sarbanes-Oxley Act of 2002.

3. Transforming IT Audit Processes to a DevOps Review

Problem: Nowadays, some nonfunctional requirements such as cybersecurity, machine learning, and blockchain are being inherently changed to functional requirements. This change will have fundamental effects on the IT audit process. For example, IT auditors will need to assess cybersecurity or blockchain requirements during the organization's system development operations (DevOps) process and change their audit program schedule to fit the DevOps schedule. This change can be a real challenge, especially for small and medium-sized audit teams that lack skills and experience with DevOps.

Solution: Internal audit could solve this problem by moving to an "IT audit as an embedded DevOps review service" model. As a result, the review processes for IT governance, risk, and controls must be embedded into the DevOps life cycle. As part of this process, an automated system may provide access to metadata. For example, an auditor could set up a software robot to collect evidence about risks related to vendor lock-in, changes in vendors, and data conversion. Similarly, gathering cloud provider metadata through RPA can enable internal audit to respond to other cloud-based risks.

Generally the business model must be clear, well-defined, mature, and well-documented when any kind of business, especially IT audit, wants to migrate to the cloud. The IT audit process also will be streamlining and maturing in the cloud as a system. Thus, the cloud and robotic process automation can bring an iterative business model in which the IT audit process is transformed into a cognitive computing system. This system could result in more affordable audit costs and enable IT auditors to perform more engagements each year based on automated best practices.

4. Mitigating IT Standards' Side Effects

Problem: Applying some IT standards is analogous to a drug interfering with other drugs and having adverse effects on a body. Without a unified medicine solution, a prescription may not provide the greatest benefits and the fewest negative effects. Likewise, internal audit should ensure the side effects of IT standards do not cause problems such as increasing compliance costs. Auditors must address two issues:

- » Deciding which sections of IT-related standards such as COBIT 5, ISO 2700, and NIST Special Publication 800-30 best conform with the organization's risk management framework.
- » Addressing conflicts and duplications among the various standards that might result in duplicate control objectives.

Solution: An automated IT audit system should use machine learning and recommendation systems to remove the similar or contradictory control objectives of IT standards. This way, the audit system can control the duplications among all of the standards' segments and use artificial intelligence to recommend an efficient and customized set of controls.

Transforming the Auditor

For automation to overcome these challenges, internal auditors must transform themselves, as well. This is an area in which IT audit specialists can help organizations find, prioritize, and invest in the right innovations to automate IT, internal audit, and cybersecurity processes. Moreover, by identifying ways to automate IT governance, risk, and controls, internal audit can help the IT function align its operations with the organization's governance and transformation processes. Ia

SEYYED MOHSEN HASHEMI, PHD, *is a research scholar at Ontario Tech University in Oshawa, Ontario.*

Risk Watch

BY ISRAEL SADU EDITED BY CHARLIE WRIGHT

CONFRONTING CLIMATE CHANGE

As more organizations recognize the economic risk posed by a warming planet, internal audit can serve as a change agent.

The adverse impacts of rising global temperatures and extreme weather conditions are becoming a front-line risk for businesses. A 2015 Economist Intelligence Unit study estimated that the value of global manageable assets at risk due to climate change could be as much as $4.2 trillion between now and 2100 in discounted, present-value terms. That is roughly on par with the total value of all the world's listed oil and gas companies. Meanwhile, increased regulation to confront climate change is gaining momentum around the world.

These trends are leading boards and executives to realize that today's climate-related decisions may dramatically impact their organizations in the future. Leaders are recognizing that the magnitude of climate change risks warrants a collective action as their impacts are widespread and not just a future threat. As a result, organizations may incur increased production costs, decreased demand, and delayed delivery of goods and services to their customers.

The growing stakeholder concern about climate change risks is creating demand for climate-competent auditors to help analyze the threats and recommend remedies. Such practitioners can help their organization address financial, process, and governance implications. Through a multipronged approach encompassing both strategic and tactical activities, internal audit can assist organizations in confronting climate change risks.

Being Climate-competent

Today, audit stakeholders are seeking answers to the basic questions about what climate change risks might impact them and the arrangements in place to mitigate them. Internal audit must adapt to these expectations and demonstrate the "insightful, proactive, and future-focused" characteristics described in The IIA's Core Principles for the Professional Practice of Internal Auditing.

Internal audit functions that conform to the International Professional Practices Framework should be qualified to audit climate change risks. To supplement their knowledge, The IIA has published the Practice Guide on Evaluating Corporate Social Responsibility/Sustainable Development.

Yet, a worrying trend in audit reports is that many auditors do not see climate change risks beyond financial risks to the business. Some internal audit functions may not include climate change risks in the audit plan because they are not considered a principal risk to the business. For example, according to the KPMG Survey of Corporate Social Responsibility Reporting 2017, 72% of large and midcap companies did not acknowledge the financial risks of climate

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

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

change. This could be because boards, executives, and internal audit lack understanding of climate change risks and their implications.

In other cases, although internal auditors may con- sider climate change risks in the audit plan, they may not understand the assumptions and estimates used in preparing the financial statements. Likewise, auditors may not comprehend the implications of climate change risks when applying existing accounting treatments and audit standards. Additionally, standard audit programs may not be helpful in assessing climate change risks, control criteria, and their potential impact. Finally, the audit team may not have climate-change risk specialists to assist the teams in focusing on key areas of concern.

Strategy and Risk Management Insight

Those internal audit functions can't ignore climate change for long. With these risks looming on the near-horizon, auditors can advise the board and management by promoting accountability in addressing climate change risks.

Internal audit can help ensure the organization is identifying, prioritizing, and remedying key climate change risks appropriately. For example, internal audit can advise on strategies for developing a process to define, monitor, and assess climate change risks. Auditors can ask management about the organization's resilience and sustainability, as well as audit the organization's sustainability report.

Another way internal audit can provide value is reviewing whether the business strategy aligns with the applicable regulatory environment. Auditors can facilitate root-cause analysis of potential regulatory noncompliance. Coordinating control self-assessment workshops can identify the areas where the organization's climate-change response strategy does not align with its business processes.

Internal auditors also should evaluate the financial and strategic implications of climate change risks. While the changes to carbon-free or low-carbon technology could pose potential financial risks, they also could result in opportunities such as alternative technologies, business processes, services, and products.

Internal audit should ensure the organization's enterprise risk management process includes an appropriate focus on climate change risks. Auditors can assist in developing a granular view of risks that can enable management to create appropriate risk management strategies. In addition, they should evaluate whether management has established benchmarks, metrics, success criteria, key performance indicators, and leading practices.

Where management is reluctant to consider climate change risks, internal audit can help change executives' attitudes by enhancing their knowledge of the risks and demonstrating how to assess and predict their impacts. In addition, internal auditors who have assisted other organizations in addressing climate change risks can share information and analysis of their experiences and promote the use of tools and systems for these purposes.

The Way Forward

The audit function should understand the climate change risks affecting the organization and be able to add value proactively, timely, and effectively. It is important to assess whether the organization fully grasps the implications of climate change risks. To move forward, internal audit should:

- Develop a consensus with the board and senior management about internal audit's role.
- Champion a focus on climate change-related risks by participating in the risk analysis process and educating management on the best practices in climate change-related governance, risks, and controls.
- Ensure the audit function has the appropriate skills to evaluate climate change risks and execute related audit engagements.
- Empower audit teams by developing appropriate tools and procedures for assessing climate change risks, capacity building through mentoring and effective onboarding, and including climate experts in the audit teams.
- Incorporate climate change risks into the organization's risk register and ensure appropriate audit units are contained in the audit universe. The chief audit executive should ensure that the identified risks are embedded in each audit engagement.

> The CAE should embed climate change risks in each audit engagement.

Climate change risks impact all of humanity. Consequently, there is much work to be done. The responsibilities of internal audit and the required skills are changing quickly. As a partner in a good governance process, the modern internal audit function can be pivotal in addressing climate change by positioning itself as an agent of change. Ia

ISRAEL SADU, PHD, CIA, CRMA, CISA, *is resident auditor with an international organization in Bonn, Germany.*

Fraud Findings

BY EMILY E. KIDD EDITED BY BRYANT RICHARDS

MUNICIPAL MISAPPROPRIATION

By exploiting legacy system knowledge, a key finance employee siphons county funds to his personal account.

Xavier County billed its residents monthly for their utility use through its finance division using in-house legacy software, which was not up to the rigors of modern billing and reconciliation processes. Unfortunately, the county had a "We have always done it this way" mindset, so there were no plans to upgrade the system. The county was collecting an average of $1.3 million each month in accounts receivables for the utility, cranking out manual receipts upon request and patching the system as needed to limp along to the next billing cycle.

The IT employee who set up the legacy platform and managed it for decades had retired, and back-of-the-house adjustments were much more difficult to achieve without his institutional knowledge. When new executive management at the county requested additional reporting from the system and management personnel asked to supplement controls, they were told that the software could not produce the reports they were asking for nor could they implement the additional controls requested. At this point, the internal audit department became aware of the software's reporting constraints and initiated a soft-monitoring project regarding the internal controls of the billing and payment process.

Because the software was incompatible with modern online processes, certain account activities could not be completed online. Instead, customers were encouraged to call the division with account concerns and other matters. The customer service line was shared by several employees in the finance division who were involved in the billing and payment process. The employees would take customer calls and process payments and adjustments within the system, as needed. Financial and county management accepted this diversity of personnel providing customer contact as a satisfactory level of segregation of duties. A few functions, however, were handled by Jeff Neeley, the most senior staff member in the division, who was familiar with the legacy software and the most effective at resolving those requests.

The division needed institutional knowledge so much that many weekends, when customer needs were high, he would come into the office and process those payments needing adjustment. It was during this time, without supervisory oversight, that Neeley conducted inappropriate transactions, feeling empowered by the lack of physical management review.

The fraud, itself, included a few adjustments to the financial software and a bit of manual tracking. When a customer paid using a credit card over the phone with Neeley, he would tally the payment amount in a

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

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

LESSONS LEARNED

- » Internal controls should be respected in all organizational cultures. Creating a baseline for oversight and applying management reviews consistently for all employees is recommended.
- » Key employees are great additions to organizations and are often the most trusted employees. They can provide institutional knowledge that can compel fact-driven decision-making. However, trust is not an internal control and all employees require oversight.
- » Succession planning and work-task rotations could have been key in preventing the fraud from occurring at the level it did.
- » By not requiring Neeley to attend staff training and enabling special working conditions, management created an environment where the employee felt outside of the system and its authority.
- » Physical security of a work area is important to instill a sense of oversight and supervisory review for employees. Working outside of normal business hours is not recommended.
- » Segregation of duties within the financial system is key to ensuring appropriate reviews. If one employee has two separate logins for staff transactions and supervisory/review transactions, this built-in internal control is no longer effective.

workbook on his desktop computer. During month-end close-out procedures, he would take the running tally amount in the workbook, create a journal entry, and move that amount from accounts receivable revenues to accounts payable. This entry was processed within the financial system without additional review as Neeley had both a staff-level login and a supervisory-level login, presumably to perform different roles for different duties, as assigned. A phony invoice was then created for a fictitious vendor and included in the backup documentation for that journal entry. The fictitious services amounted to the total of all individual accounts that were manipulated during the month. The vendor was paid via the standard accounts payable process within the county. The vendor verification process had been completed by Neeley many years before.

Through multiple inquiries during performance audits throughout the organization, internal audit identified a weakened internal control structure due to the level of trust within the county. Internal audit discussed the risks multiple times with executive management, with no change. In fact, when internal auditors cautioned against this untested trust, they were told it was important not to upset employees because they were still skeptical of the county after layoffs during the Great Recession. Those who remained were territorial regarding their responsibilities and did not see the value of cross-training.

The utility's legacy system led to the practice of a few key employees handling adjustments every time one was needed. The work became so specialized that certain cus- tomer account adjustments were put on hold until Neeley returned to work. It wasn't until he was out on unscheduled medical leave that another person within the department had to handle his transactions for waiting customers. That's when personnel noticed unusual adjustments within the system.

Adjustments within the monthly journal were paid via the accounts payable process to a fictitious service vendor account Neeley set up many years before that appeared to be a legitimate cost of service as payment lockbox service fees. This service fee was one of two that the county paid—because the fee amounts were consistent, without material variances, and of a nominal amount, no one thought to ask why there were two separate payments for the lockbox service fee.

Once the fraud was identified, internal audit asked the employees who reviewed Neeley's summary reports why the fictitious vendor account wasn't flagged or reviewed further. They explained that it did not receive any attention because the fee was nominal considering the large amounts that were being processed monthly. The fraud investigation determined that those nominal fees siphoned to Neeley's personal account added up to nearly $91,000 and, because the system did not retain records more than 10 years back, the true dollar amount lost by the county was estimated to be greater.

The department was informed of the suspected fraud, and a vendor service company conducted a financial investigation. Still out on medical leave, Neeley hastily completed retirement paperwork with human resources and did not return to work. The investigation resulted in multiple recommendations that brought the division back up to an appropriate level of internal control. The county later submitted the case to the local district attorney's office for prosecution, which is currently in process.

The impact to the county was perhaps greater than the monetary loss of the fraud. It became a local media topic, drawing many concerned citizens to the county's public meetings to voice their disproval of the situation and the county. The level of trust in the community has been eroded and it will take time to mend. Ia

EMILY E. KIDD, CIA, CGAP, *is director of internal audit for the City of Reno, Nev.*

EMERGING

This year's honorees are driving change in their audit functions and setting an example for the profession.

LEADERS 2019

Russell A. Jackson

Each year's Emerging Leaders talk less about the profession pivoting to a trusted advisor role and more about actually performing that role—and how excited they are to expand internal audit's influence into new areas. Indeed, the 2019 Emerging Leaders' diversity shows partly in the variety of experiences they've had in an advisory capacity and their specific goals for expanding the profession's profile. And as in previous years, the 2019 Emerging Leaders are a diverse, multinational group. Since the first crop of honorees in 2013, 14 countries have been represented; this year's professionals hail from The Republic of Belarus, Canada, the U.S., and Zambia. Just under half since the beginning are women, just over half are men—many of whom have advanced to positions of greater leadership and gone on to volunteer in key IIA governance and advisory positions.

As a group, this year's Emerging Leaders are enthusiastic about talking up internal auditing—to schools, business groups, and their colleagues—and about supporting the profession through expanded participation in local professional organizations. Technology, as always, is what these high-performing practitioners want to talk about. Automation and data analytics are familiar. In fact, emphasizing analytics seems almost old-fashioned to the 2019 honorees; they assume analytics are key to internal auditing and continually expand their skills—often on their own time. That expertise opens doors to more internal auditor interaction with organizations' executives, and this year's Emerging Leaders are eager to take advantage of the opportunities they see ahead to be meaningful players in their enterprises' success.

JORDAN SWEENEY

CFE
28
SENIOR AUDITOR
CITY OF SACRAMENTO, CALIF.

JORDAN SWEENEY conducts "impactful audits," as one colleague puts it, and she is hailed for following up to ensure recommendations are implemented. From day one, the University of California at Davis graduate was given sole responsibility for auditing the city's Department of Utilities (DOU). As a result of her consistent follow-up efforts, the DOU has achieved "a realized monetary benefit of more than $15.2 million dollars," reports Sweeney's supervisor, Sacramento Assistant City Auditor Lynn Bashaw. "She continues to work with the department to implement recommendations made in her audits," Bashaw adds, "as well as recommendations made in previous audits." Sweeney says providing informal audit training to DOU staff members responsible for the recommendation follow-up efforts helps them understand what internal audit is looking for and communicate that to other staff, thereby reducing the number of documentation requests she has to submit. She also manages the city's whistleblower hotline for reporting fraud, waste, or abuse, and so far has resolved more than 80 cases. Sweeney, who holds a master's degree in civil engineering, came to the profession after learning about it at home—her husband is a premium auditor for an insurance company. The work seemed challenging yet fun, she explains, and used many of the same data analysis and problem-solving skills an engineering education requires. Sweeney adds: "I felt it would be very rewarding to be a part of something with such a big impact on how the government operates."

CHENG CHENG

CIA
28
CONSULTANT, ENTERPRISE RISK SERVICE
MNP LLP
TORONTO

This is how **CHENG CHENG** characterizes his profession: "I selected internal auditing because it's challenging, nonroutine, and fun." The University of Toronto graduate started out with a degree in commerce and a master's degree in accounting; early in his career, Cheng worked on finance, assurance, and internal audit-related jobs, ultimately opting for the latter as his main focus. "Every day is a new challenge and learning opportunity," he says. One early challenge was how dependent consulting is on experience and industry knowledge, which he lacked at the time. "I forced myself out of my comfort zone," he says. "I told myself, 'Don't' be afraid to ask questions.'" And having tapped his mentor's experience to great effect, he advises those working with professionals who have extensive knowledge in the field to observe how they work. Cheng's own work encompasses internal controls over financial report- ing, payroll audits, external quality assessment, and risk-based operational and compliance audits, notes MNP colleague Jim Barbour, who cites another challenge Cheng has overcome. "A recent client required him to reconstruct multiple years' payroll reporting to tax authorities," Barbour says. "He used document capture and data analytics tools to prepare and evaluate the source data for the required deliverables." Cheng points to the value of communication skills as key to explaining deliverables to clients. "No matter how technology evolves," he says, "we will always need to build relationships with people." Outside internal audit, pick-up basketball games most weekends constitute Cheng's No. 1 hobby. He's also an active volunteer in MNP's Community Activity Project and Education program and serves as treasurer for IIA–Toronto.

"I'M REALLY CONFIDENT OUR PROFESSION IS IN GREAT HANDS WITH SO MANY INTELLIGENT AND SOCIALLY CONSCIOUS YOUNG PROFESSIONALS." —Sally-Anne Pitt, Emerging Leaders judge

BLAINE FRITZ
CIA
29
GOVERNANCE & OPERATIONS MANAGER/ CHIEF OF STAFF
GSK
RESEARCH TRIANGLE PARK, N.C.

BLAINE FRITZ became an internal auditor to understand how companies work from the inside out. He hit the professional jackpot: The Michigan State University graduate has led global audit teams and conducted engagements across multiple risks—commercial practices, anti-bribery and corruption, financial controls and reporting, and supply chain, to name a few. His work has spanned multiple functions, cultures, and geographies, including North and South America, Europe, and Asia. The former audit manager, who's since moved into Managed Markets and Government Affairs, has also led multiple initiatives to improve the internal audit function at GSK, notes his manager, John Boone, vice president, Contract Management and Operations. "He's gathering observations on the impact of an audit from a business perspective," Boone says, "and will feed these observations back into the internal audit function to improve efficiency and effectiveness and minimize business disruption in future audits." Other projects include leading the Audit Ways of Working Alignment Project, which identified differences in approach between regions and among risk areas, and facilitating training on audit process and third-party oversight. The people part of the equation, Fritz says, is key. "My work provides an opportunity to gain a global perspective and cultural awareness through the people I meet around the world," he says. Fritz focuses on internal audit's evolving role, noting that use of the audit function as a resource for insights gained through sharing of good practices across the business represents an important change for the profession. "Auditors can share an enterprise view gained from experiences in different risks and parts of the business," he comments. Outside the office, the soccer player and youth team coach also serves as an Early Talent Mentor for GSK's Future Leaders Program and as a member of GSK's Orange Day Volunteer Committee; each year, employees spend Orange Day off-site, volunteering at a charity of their choosing.

MELISSA MORLAN DONNER prefers people to face forward in their approach to internal auditing. "If 'well, that's how we did it last year' is the only rationale you have for something," she says, "there's probably a way to improve it." That often involves automation and, especially, being able to understand what it's doing. Already, the University of Florida graduate notes, a key skill for internal auditors is "the ability to understand how automation can be applied." Writing code is a plus for anyone to possess, she says. "But more important is being able to clearly articulate what you think an automated process would look like and have a grasp of what is possible before working with an automation expert to get it done." Donner built her audit skills analyzing and testing controls across various industries as a consultant, while also project managing the day-to-day activities of those engagements, reports current supervisor Janet Jarnagin, an audit director at Bank of America. Now Donner is responsible for board and executive management reporting, including presentations summarizing audit results, issue status, and audit department performance to the organization's highest governing bodies, Jarnagin says. Within months of starting at Bank of America, Donner designed a new monthly business review for the chief audit executive (CAE) to oversee department operations and revamped the issue management report for the CEO's management team. Donner says that's a good example of the trusted advisor role internal audit is taking on, and she adds that data visualization is an increasingly important part of it. Reporting a 1% to 2% month-over-month increase via text or a slide may not raise red flags, she explains. But seeing a line chart spanning six months that shows a 10%-plus increase—with a six-month projection if nothing happens—"can really serve as a call to action," she says. Donner is a member of The IIA's Chicago chapter and volunteers at TutorMate, an online program that helps kids improve their reading skills.

MELISSA MORLAN DONNER
CIA
26
AUDIT SUPERVISOR
BANK OF AMERICA
CHICAGO

15th Annual

The 2020 Atlanta IIA Conference

September 11, 2020

CONGRATS MEGAN BEESTON

2019 EMERGING LEADER

Megan Beeston earned her IAEP at the KSU in 2016, where now she volunteer teaches IA.

Megan Beeston takes her place among the leaders of the IIA Atlanta Chapter by winning the Chapter's Mulcahy Leadership Award. Shown here with other 2019 MLA winners John Greene, Michelle Chelemer (also a 2018 IA Magazine Emerging Leader), Emil Tzanov, and Delores White. Also shown Bill Mulcahy, IIA Atlanta Chapter President and IIA NA Chair Karen Brady.

Megan Beeston (far right) is leader of the Young Professionals training session at The IIA Atlanta Conference. Shown here with her expert panel of Young Professional Leaders, Delores White, Chair of the Chapter's mentorship program, Stefanie Chambers, Member of an IIA Global Committee, and Thomas Sherrill, 2018 IA Magazine Emerging Leader.

The IIA Atlanta Chapter's mission is to be the premier professional association dedicated to the promotion, advocacy, and development of the practice of internal auditing in the Greater Atlanta Metropolitan Area. This shall include, but is not limited to, the following: Professional development, promotion of IIA certifications, internal audit research and information sharing, and working with universities to promote internal audit education. The IIA Atlanta Chapter worked with Kennesaw State University and Georgia State University to establish IIA Internal Audit Educational Programs (IAEP) at both universities.

KENSON MUNSHYA

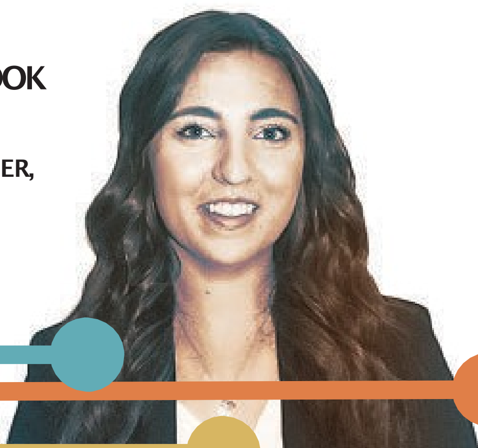
CIA, CISA
29
AUDIT MANAGER
STANBIC BANK ZAMBIA
LUSAKA

KENSON MUNSHYA first saw internal audit from the outside, and found himself impressed by practitioners' insights and deep understanding of the organizations he was auditing externally. "Over time," the Rusangu University Zambia graduate says, "I started looking at the internal auditors' reports as one of the reference points to gain an understanding of clients." Then he joined them—and started spreading the word about internal auditing. "He has a mission to make a difference in the profession," says colleague Chuma Silutongwe. He adds that Munshya was instrumental in helping parent company Standard Bank Group's Africa regions team win the firm's 2018 Group Internal Audit Mark of Excellence Award for enhancing the use of data analytics and audit automation. Plus, he's supported teams from Namibia, Malawi, Botswana, and Mauritius in providing key insight on IT-related engagements, such as cybersecurity and business continuity audits. Munshya says practitioners need to prepare for the future by improving their skills in data analytics, machine learning, and artificial intelligence (AI); he is piloting the automation of the company's audit process using those very skills. Still, he adds, "ultimately, it comes down to one's people skills to manage change and influence decisions." Internal auditing often involves negotiating with management, so a firm grasp of the disruptive technologies combined with people skills is key, Munshya stresses. "I'm amazed at internal audit's ability to influence an organization and be a change agent around strategy and operations, as well as around governance, risk, and internal controls," he says. Outside of internal audit, Munshya enjoys decidedly low-tech pastimes, including chess, jogging, and reading. He also volunteers for outreach programs through his church and is an active member of IIA–Zambia.

MADDIE COOK is in the enviable position of working in a role that requires her to indulge in one of her favorite pastimes. The job requires travel, and Cook says, "I really enjoy learning about the cultures that are new to me and sampling local cuisine." And her travels provide valuable insights for her global client work, notes Pamela Hrubey, a Crowe managing director and Cook's career coach. "She leverages the business experience she has gained from working in Canada and the United States to support a variety of clients with offices around the globe," Hrubey says, "bringing a balanced business perspective along with her deep knowledge of internal controls." The University of Western Ontario graduate is also part of an innovation team considering ways to leverage blockchain technology to create internal audit efficiencies, and she's been researching the potential of robotic process automation and AI. "Clearly we will see, over time, these technologies playing a large role within our profession," she comments. To assess controls around that technology, internal auditors will need a robust understanding of how it functions, the associated risks, and the organization's strategy for integrating the technology into its business processes. "The more knowledge we have, the better we will be able to assist, review, and potentially advise management on implementation in the future," Cook says. She also points to significant opportunity to use these technologies in audit work. Companies are making the move to blockchain and other technologies to advance their businesses, she notes. "Internal auditors will need to adapt our methodologies to maximize the associated benefits of the new tools by developing audit programs that increase organizations' confidence in their use." Outside the profession, Cook has donated her time to the Boys & Girls Club of America, a community food bank, and an organization that builds bikes for kids.

MADDIE COOK

CPA
30
SENIOR MANAGER, CONSULTING
CROWE LLP
LOS ANGELES



JIAHUI "BELLA" WANG

CIA
28
SENIOR INTERNAL AUDITOR, COMPUTER INFORMATION ANALYST
ATLAS AIR INC.
PURCHASE, N.Y.

BELLA WANG was surprised to learn how much soft skills support the technical aspects of internal auditing. "I didn't understand the diversity of attributes a practitioner needs to have to be effective," the St. John's University graduate explains. In particular, Wang says that recognizing the importance of sales skills was a professional "aha!" moment. "We are selling our expertise, ideas, and recommendations almost every day to help add value to our organizations." Wang accomplishes that with a firm foundation of technical knowledge, says her supervisor, Charles Windeknecht, Atlas Air's vice president, Internal Audit. "She consistently exhibits a deep understanding of the risk and control considerations she is assessing," he says, "by asking challenging questions in a relevant and meaningful manner." The questions change, of course, as the technology that powers the profession changes. "Technology and automation will make changes in how, where, and when we perform audits," Wang says. Already, she has designed and built several data analytics programs to support internal audit's objective of executing more effective testing, Windeknecht notes. Wang says her department uses analytics routines during annual fraud assessments to help management isolate higher risk transactions. "Senior management is coming to us with more requests to help them identify process improvement opportunities," she says. Wang is also active with the youth education nonprofit Junior Achievement and often speaks at area college and university events about the benefits of internal auditing.

MEGAN BEESTON

CFE
29
PRG SENIOR ASSOCIATE
FRAZIER & DEETER LLC
ATLANTA

Stephen Brown, CAE at PRGX Global, recalls the time **MEGAN BEESTON** was working on an IT project for his company as part of a co-sourced team when her supervisor was injured and unavailable for an extended period. "Megan stepped up and successfully managed the project with minimal oversight, and exceeded expectations in every way," Brown says. The Kennesaw State University graduate says the experience provided her tremendous opportunity for learning and growth. "Working in public accounting constantly involves quickly and seamlessly adapting to unexpected situations to avoid delays in projects and deadlines," she says. She benefitted from having built good relationships with clients—and having the ear of her company's managers. Early on, she says, she stepped back and realized that internal audit has long used data analytics. But the progress underway now is even more exciting, she adds, as technology increasingly enables internal auditors to expand their capabilities past current roles. "Integrating IT concepts into our strategies will allow us to provide the most value-add to our organizations," she says. "Any initiative for research or training in technology and how we can apply systems to be more efficient is an important step for us." Beeston came to the profession when a professor presented it in a compelling way—making her realize she could use people skills to make her role more successful and help people solve problems, which she saw as a perfect fit. Her internship exposed her to a variety of roles and projects, piquing her interest even further. "The ability to wear many hats—as an extension of an organization as its internal audit function, as a service auditor, or consulting through process improvements and security assessments—challenges me technically and as a person," she says. Outside internal audit, Beeston plays tennis and watches college football. She also fundraises for the Leukemia & Lymphoma Society through her company, volunteers on select weekends with the pediatric grief counseling organization Kate's Club, and co-chairs the mentor–mentee program at her local IIA chapter.

AIDAR ORUNKHANOV

29
SOLUTIONS DIRECTOR
TAMR
CAMBRIDGE, MASS.

AIDAR ORUNKHANOV approaches internal audit from a different perspective. The University of Illinois at Urbana–Champaign graduate started out in data analytics and came across internal auditing by chance. But he noticed that the profession was beginning to implement data-driven methodologies and saw the potential to implement analytics. He's now back in data analytics, at a start-up that applies machine learning to data unification, but comments that the massive amounts of data produced by new technology will propel internal auditing toward near-real-time functional- ity and other elements of automation, raising some worries about technology replacing humans. But he says the technology can't replace humans completely: "I'd call it 'using new tools' rather than 'managing robotic assets.' Robotic process automation [RPA] is an ideal solution to frequently repeated rule-based processes." RPA, in fact, should free up time for more creative and exciting work, he says. One example: He led development of an automated dashboard at a former employer that provides auditors with timely changes to risk profiles and data-enabled outliers for testing purposes. He also co-led a hands-on data analytics training program for 200 colleagues. In addition, Orunkhanov lectures at Boston University, teaching a graduate-level course in business analytics. On weekends, he enjoys travel photography. "The gear I carry has grown exponentially," he says," but an incredible Instagram picture is worth it all." Orunkhanov also volunteers at a local food bank and helps families file their tax returns.

After a stint in external audit, **MARILYN CARNEVALE** has been happily surprised by how gratifying she's found her internal audit career—particularly the newness of each assignment. "Internal audit procedures often have to be developed from scratch to meet the unique needs of an organization," she says. "It's exceptionally challenging, but completely rewarding when our recommendations come to fruition." At Rutgers, her alma mater, Carnevale was assigned to assist on "a major, multi-phased project," reports her supervisor, Marion Candrea, manager, Audit and Advisory Services. "It was part of a highly regulated area that required a rigorous learning curve that she easily overcame," Candrea says, adding that Carnevale started taking on lead auditor tasks right away. With that responsibility came the opportunity to work with student interns. In fact, she was so effective that she soon earned the title of internship program supervisor. Carnevale remembers people leaving her former public accounting firm for internal audit positions, but adds now: "Honestly, I did not even know if I would be any good at it." Her ties to the university moved her to pursue the position she's in. "The fact that I'd never heard of internal auditing until about four years into my career is partially why I believe in advocating for the profession," she says. That includes educating students about options beyond public accounting. In her free time, Carnevale volunteers at The IIA's Central Jersey Chapter, attends Rutgers athletics events, donates her hair to Locks of Love and Pantene Beautiful Lengths—and plays the piano.

MARILYN CARNEVALE

CIA, CPA
30
SENIOR AUDITOR RUTGERS, THE STATE UNIVERSITY OF NEW JERSEY PISCATAWAY, N.J.

"THIS YEAR'S HONOREES ARE MOTIVATED INDIVIDUALS WHO UNDERSTAND THE VALUE OF THE CIA CERTIFICATION AND THE COMMITMENT TO MAKE A DIFFERENCE IN THEIR ORGANIZATIONS THROUGH THIS GREAT PROFESSION." —Michael Fucilli, Emerging Leaders judge

CHRISTOPHER BALLWEG

CIA, CISA
28
IT AUDIT SUPERVISOR
AMERICAN FINANCIAL GROUP INC.
CINCINNATI

No matter how much internal audit technology advances, success in the profession will always rely on people skills, according to **CHRISTOPHER BALLWEG**. With a primary focus on IT audits, he sees technological advancements as key to driving change—but the University of Kentucky graduate also stresses that "relationship-building, clear communication, and adaptability" are a practitioners' most important competencies. Indeed, he says, auditors must be able to clearly communicate any questions or observations, regardless of the business partner. Education helps. Ballweg started at American Financial Group right out of college, notes former colleague Brian McNalley, IT audit manager at Macy's and a 2018 Emerg- ing Leader. Since then, he has received two key professional certifications and an MBA from Mount St. Joseph University. On the job, Ballweg has been a team leader for engagements involving cybersecurity, disaster recovery, business continuity, the Payment Card Industry Data Security Standard, and U.S. Sarbanes-Oxley Act of 2002 compliance. "A key challenge is ensuring that our work is adding value to our various stakeholders," Ballweg says. Practitioners who want to be seen as trusted advisors, he adds, must know stakeholders' goals and ensure that engagements are focused on delivering value. That, he says, requires flexibility. "Continuous change is the aspect of the profession I enjoy most," he says. When he started, cybersecurity audits and the U.S. National Institute of Standards and Technology Cybersecurity Framework were "still in their infancy," he says. "Now they're on the mind of nearly every stakeholder in an organization." Ballweg has been active in The IIA's Cincinnati Chapter since 2013, and is a board member of his local American Cancer Society Young Professionals group.

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

CHRISTIANE DOLORES

29
INTERNAL AUDIT MANAGER
CAESARS ENTERTAINMENT CORP.
LAS VEGAS

Today's students at the University of Nevada Las Vegas have access to a career insight that **CHRISTIANE DOLORES** didn't. The alumna makes a point to attend events on campus to meet students and engage them in the internal audit community, she says, because most of her time as a student was spent learning about external auditing. She's become deeply involved in the profession, having served on the IIA–Las Vegas board as secretary, vice president of Programs, and now vice president, notes her supervisor, Victor Echenique, Caesars' internal audit director. Dolores led an awareness initiative about the services internal audit provides and created a brochure for Internal Audit Awareness Month that was distributed to 145 colleagues throughout the Caesars organization. She excels at her job, Echenique says, winning the "Audit Ninja" title as internal audit's Employee of the Quarter and Employee of the Year six times in a department of more than 80 practitioners. She manages planning and execution of compliance, financial, and operational audits of business opera- tions at casino properties in multiple states, and she's a leader in the department's philanthropy efforts. Dolores didn't set out to be an internal auditor, starting her career in Accounts Receivable and moving around the enterprise to learn several different accounting functions in the organization's nongaming enterprises. "I had no intention of working for internal audit," she says. Then, conversations with a colleague helped change her mind. Now she calls it "probably the best decision I've made for myself."

> **I WAS IMPRESSED BY THE LEVEL OF COMMITMENT THESE EARLY CAREER HONOREES HAVE TO THE INTERNAL AUDIT PROFESSION, DEMONSTRATED BY ACTIVE IIA INVOLVEMENT AND INVESTMENT IN THEIR RESPECTIVE TEAMS.** —Thomas Sanglier, Emerging Leaders judge

KATSIARYNA PRANOVICH has learned the value of listening. Early on, she found communicating with internal clients to be "the most laborious, difficult aspect of the job." But then she learned to listen more attentively to her colleagues, she says, to focus better on what they need from her. "That, plus gaining experience and exercising patience allowed me to adjust my style of communication," she explains. Pranovich sharpens her people and public speaking skills with stand-up performances of her own comedy material in local clubs and cafes. One of her favorite parts of the job, the Belarusian State Technical University graduate emphasizes, is helping colleagues deal with difficult situations. Another is the opportunity to "engage in different areas of the organization's activi- ties." Pranovich extends her internal audit interactions outside the enterprise as well, notes Pavel Varyvonchyk, CAE at JSC MTBank. "She constantly expands her professional skills by attending seminars and conferences," he says, "which allows her to maintain professional relations with internal auditors at similar companies here and in neighboring countries." Indeed, Varyvonchyk adds, Pranovich is a two-time winner of the firm's Best Employee Award. One reason is her involvement in a project examining data mining for automated internal auditing, which aims for continuous monitoring of key departmental indicators of possible process violations. Another project Pranovich heads up is creating automated workpapers and options for management decision-making following audits. Pranovich is, in fact, lauded for her methodologically accurate documents. "The devil is in the details," she says, "especially with the increasing speed of work and changes in business processes."

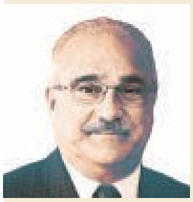
KATSIARYNA PRANOVICH
29
CHIEF AUDITOR
JSC MTBANK
MINSK REPUBLIC OF BELARUS

STEVE SPITTLER
CPA, CISA
28
SENIOR IT INTERNAL AUDITOR
LPL FINANCIAL
FORT MILL, S.C.

STEVE SPITTLER is a technology enthusiast with strong people skills—two important assets for an internal auditor specializing in IT engagements. "As companies move to the cloud and increase use of third-party vendors," says the Bentley University graduate, "even practitioners who mainly perform business or compliance audits need to understand the implications cybersecurity could have on their engagements." Nearly every audit his team performs has cybersecurity considerations, he notes. A recent challenge involved leading both the Vendor SOC1 testing program and the cybersecurity audit for the enterprise, reports co-worker and unofficial mentee Anja Erlandson, senior analyst, risk management, at LPL. "He not only completed the tasks," she says, "he assisted the business in creating new internal controls, making recommendations consistent with industry best practices." He also has added visual analytics to audit reports, analyzed large data sets to identify discrepancies, and tested the effectiveness of department policies and procedures. The first few years of Spittler's career were spent as a public accountant conducting external financial audits; he says the move to his current post represented an opportunity to grow his skills. His social network also has expanded. Spittler says: "What I love about my job is the level of collaboration and the people." Most of his engagements are integrated, with the business audit and IT audit teams working together, he notes, citing the value of building relationships with clients. Practitioners often can see firsthand the improvements made because of their recommendations, he adds. Off the clock, Spittler volunteers at the Humane Society, the Metrolina Food Bank, and the Boys & Girls Club of America.

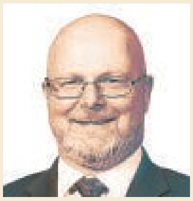
Meet the Judges

According to this year's judges, the 2019 Emerging Leaders deserve recognition for their innovative thinking, service to the profession, and considerable IT expertise. Many, in fact, are "driving digital change in their audit functions," as one judge put it. The distinguished group of judges, who hail from a range of organizations and backgrounds, also point to the honorees' impressive array of business, audit, and communication skills.



MICHAEL FUCILLI, CIA, QIAL, CGAP, CRMA, auditor general, Metropolitan Transportation Authority, New York; director, Research, IIA Global Board of Directors

SALLY-ANNE PITT, CIA, CGAP, managing director, Pitt Group Pty Ltd., Richmond, Victoria, Australia; director, Professional Practices, IIA Global Board of Directors



THOMAS SANGLIER, CIA, CRMA, CPA, internal audit director, Raytheon Co., Waltham, Mass.; vice chairman, Specialty Groups, IIA North American Board of Directors

JULIE LATHROP, CIA, CRMA, CPA, North American controller, HP Inc., Houston; director, Professional Certifications, IIA Global Board of Directors; vice chair, Finance, IIA North American Board of Directors

WADE CASSELS, CIA, CCSA, CRMA, senior IT auditor, Nielsen, Lakeland, Fla.; member, IIA Publications Advisory Committee

KARIN HILL, CIA, CGAP, CRMA, former director of Internal Audit, Texas Health and Human Services Commission, Austin, Texas; member, IIA Publications Advisory Committee

SARAH MURRAY

CIA

27

SENIOR AUDITOR

SAVANNAH RIVER NUCLEAR SOLUTIONS

AIKEN, S.C.

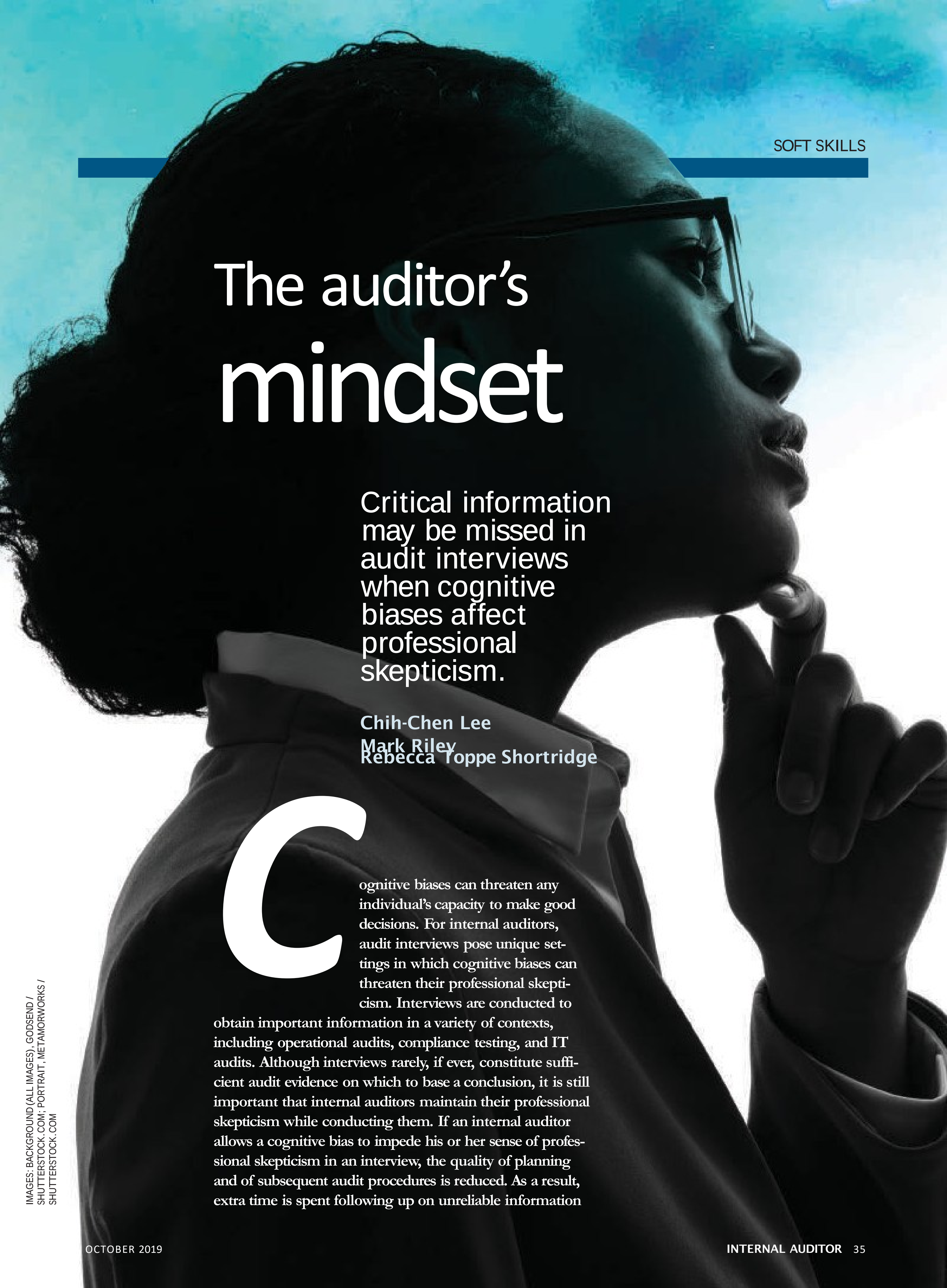
For **SARAH MURRAY,** early career inspiration came from an audit class project that involved creating flowcharts and identifying control deficiencies. "It was totally different than anything I had done in my accounting studies thus far," she says. The Augusta University graduate enjoyed it enough to apply for an internal audit internship and ended up "falling in love with the work and the variety of people that you get to meet." One part of the job she's especially fond of is working with data. "It always has a story to tell you," she notes. Former Augusta University accounting lecturer and current colleague Steve Loflin, principal internal auditor at Savannah River Nuclear Solutions, says Murray's skills in analytical and substantive testing are exceptionally advanced. "As much as she impressed me as a student," he comments, "I've been even more impressed by her abilities as an internal auditor." Loflin adds that Murray is known for her timely and effective auditing and her ability to build relationships. Murray does have an agenda: She's out to end the "gotcha" and "take no prisoners" stereotypes of internal auditors. She makes a point to find ways to minimize nervous tension during engagements by checking clients' work spaces for clues to a favorite football team or new grandchildren. "I get them talking about those things to loosen them up," she notes, "and see audit as a function that is truly there to help." Murray also volunteers with local youth ministries, and with the River of Life, which provides exterior home repairs and improvements to local community members. In addition, she's active in, and a former officer of, The IIA's Central Savannah River Area Chapter.

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

Congratulations!

To our own Maddie Cook, a senior manager in our consulting group. Maddie has been recognized as an emerging leader by her coworkers and by the Institute of Internal Auditors. Maddie's smart decisions today provide lasting value to clients and coworkers.

crowe.com



The auditor's mindset

Critical information may be missed in audit interviews when cognitive biases affect professional skepticism.

Chih-Chen Lee
Mark Riley
Rebecca Toppe Shortridge

Cognitive biases can threaten any individual's capacity to make good decisions. For internal auditors, audit interviews pose unique settings in which cognitive biases can threaten their professional skepticism. Interviews are conducted to obtain important information in a variety of contexts, including operational audits, compliance testing, and IT audits. Although interviews rarely, if ever, constitute sufficient audit evidence on which to base a conclusion, it is still important that internal auditors maintain their professional skepticism while conducting them. If an internal auditor allows a cognitive bias to impede his or her sense of professional skepticism in an interview, the quality of planning and of subsequent audit procedures is reduced. As a result, extra time is spent following up on unreliable information

IMAGES: BACKGROUND (ALL IMAGES), GODSEND / SHUTTERSTOCK.COM; PORTRAIT, METAMORWORKS / SHUTTERSTOCK.COM

DESCRIPTION AS TRUTH

During an internal audit team's first day on site at a parts distribution center, it requests a walk-through of the facility to gain an understanding of the intake, storage, inventory, and shipment of parts. A floor manager walks the team members through the facility explaining and answering their questions about each process. Based on the floor manager's explanations and answers, the team identifies the high-risk processes and develops testing procedures for those processes. On the third day of the visit, the auditors begin testing the inventory process and note that each test is failing. During the results validation meeting with the general manager, the team learns the inventory processes described by the floor manager were incorrect. Because the auditors accepted the floor manager's description as the truth, they had to recreate and reperform the inventory testing. In hindsight, professional skepticism would dictate that the internal audit team had no basis on which to trust the floor man- ager's explanations as credible. Before identifying high-risk processes and designing and carrying out tests, the team should have taken additional steps, such as corroborating the explanations with documented evidence of transactions. Asking themselves if they were comfortable basing several days of work solely on the explanations of one person who they had just met could have saved the team significant time and effort.

ALEXY_M / SHUTTERSTOCK.COM

or, worse, important information is missed. Three biases, in particular, may affect internal auditors' profes- sional skepticism: truth bias, confirma- tion bias, and the halo effect.

TRUTH BIAS

The assumption that others are telling the truth is necessary on a day-to-day basis to facilitate routine social interaction. If one tried to verify the truthfulness of every statement made by others, routine communication would grind to a halt. However, the tendency to believe others are providing truthful information may prevent internal auditors from employing appropriate levels of professional skepticism, which entails, at a minimum, a belief that sources of information are neither truthful nor untruthful. Truth bias has been documented repeatedly in deception detection research and seems to be a major factor limiting people's ability to detect false statements in a variety of settings. The assumption of truthfulness is a common bias that may impede effective decision-making and, by extension, professional skepticism.

To combat truth bias, internal auditors should remain aware that the profession requires a questioning mind. By definition, truth bias involves a deficient use of questions and additional procedures just when they are needed most. When relying on information obtained in an interview, it is imperative that internal auditors ask themselves whether they employed a critical mindset in assessing the information they received, in posing follow-up questions, and in obtaining corroborating information. If not, then truth bias may have impeded professional skepticism (see "Description as Truth" on this page). The findings in Norah Dunbar's, Artemio Ramirez Jr.'s, and Judee Burgoon's Winter 2003 *Communication Reports* article, "The Effects of Participation on the Ability to Judge Deceit," suggest that interviewers should work in pairs, with one interviewer performing the questioning, while the other member of the team observes. Dunbar and her co-authors find that the observer in such scenarios is better able to judge deceit on the part of the interviewee.

CONFIRMATION BIAS

When one seeks out or gives too much weight to information consistent with a specific belief, that is confirmation bias at work. It may influence questions asked and how the answers received during an interview are processed. Internal auditors conducting interviews can certainly fall victim to confirmation bias by seeking out information consistent with a specific belief during those interviews. Often, this involves seeking out information that processes are operating as they should. Confirmation bias has the potential to compromise an internal auditor's

Skepticism is about **quality**, not quantity—asking the **right questions**, according to The Institute of Chartered Accountants in England and Wales' Skepticism: The Practitioner's Take.

professional skepticism by steering the auditor toward a particular conclusion, regardless of the facts.

In their June 2011 *Harvard Business Review* article, "The Big Idea: Before You Make That Big Decision…" Daniel Kahneman, Dan Lovallo, and Olivier Sibony suggest managers combat confirmation bias by asking teams that are making recommendations whether credible alternatives to their recommendations have been considered. Interviewers should engage in a similar process.

To combat confirmation bias in an interview setting, internal auditors should enter with a conscious openness to learning about or uncovering information that is inconsistent with their prior beliefs. After the interview, they should ask themselves whether they learned anything that was contrary to their prior beliefs and whether they missed any opportunities to ask follow-up questions that would have uncovered such information. In other words, as Kahneman and his co-authors recommend, consider credible alternatives. Such an approach is consistent with professional skepticism. If the auditor in the "Seeking Information as Confirmation" example on this page had entered, conducted, and reflected upon her interview with such an attitude, she would have been more likely to focus on the exception that was apparent in the business finance manager's response.

SEEKING INFORMATION AS CONFIRMATION

An inexperienced internal auditor meets with a business finance manager to understand how payments are received from clients and processed. In preparation for the interview, the auditor creates an agenda containing a list of questions. During the interview the auditor asks, "What do you do with checks you receive from clients?" The business finance manager replies, "I deposit most of the checks into the company account." Without hesitation, the auditor asks the next question on the agenda. She likely has a bias toward finding that the checks are all deposited in the correct bank account. By ignoring the phrase "most of the checks," the auditor fails to detect that the business finance manager is depositing some checks in inappropriate accounts. In fact, during the course of the audit, it becomes apparent that the finance manager and other persons are depositing some of the checks in their manager's personal account for department parties and outings. The account owner and the persons making the deposits are ultimately terminated. By seeking out information consistent with what she knew should happen, the internal auditor who conducted the interview initially missed the fact that some checks were processed inappropriately, increasing the possibility that the audit could have missed this fact entirely.

THE HALO EFFECT

In the book *Thinking Fast and Slow,* author Daniel Kahneman describes the *halo effect* as the "tendency to like (or dislike) everything about a person—including things you have not observed." Internal auditors should be aware of the biases created by the halo effect. If they like someone or view him or her favorably, they might tend to weigh their opinions and estimates on all topics more heavily than they should. On the other hand, if they do not like a person, they may have a bias in the opposite direction. Either way, they are checking their professional skepticism at the door.

Kahneman suggests fighting the biases created by the halo effect by verifying information using independent sources. In "The Weight of Credentials" example on page 38, had the halo effect not compromised the auditors' professional skepticism, they might have been able to corroborate the information provided by the gemologist with independent sources. Such sources should have included additional interviews, as well as documentation. By taking such steps, they

Considering credible alternatives is consistent with professional skepticism.

THE WEIGHT OF CREDENTIALS

An internal audit team was auditing the jewelry return process at a merchandise return center. When the team inquired about the smelting and gemstone procedures, it was referred to the director of jewelry, who also was a licensed gemologist. During the interview, the gemologist was knowledgeable, friendly, and eager to share everything that was working well and everything needing to be improved. As a result, the team viewed him quite favorably. Although some of his process descriptions did not make sense, the team members took the gemologist's descriptions as accurate because he appeared happy they were there to help him fix all of his processes and, after all, he was a licensed gemologist. Nine months after the audit, the gemologist was arrested for selling gemstones to overseas buyers and depositing the money into his personal account. The auditors should have gathered additional evidence to corroborate the gemologist's explanations about the jewelry return process, but they were blinded by his credentials and knowledge of jewels. They fell prey to the halo effect.

could have identified the error instead of relying on the statements from someone perceived as having a halo. There were likely others involved in the processes described by the gemologist who could have discredited his statements. Although there is no guarantee the auditors would have detected the gemologist's scheme if they had sought out independent sources, they certainly would have increased their chances of detecting information that would have prompted them to take additional steps to further investigate the processes.

KNOWLEDGE IS POWER

There are several concrete steps auditors can take to fight the negative effects cognitive biases have on audit interviews. In addition to conducting interviews in pairs, auditors should ask follow-up questions. This can help auditors gain valuable information during interviews. Next, they should obtain corroborating interview evidence by speaking to multiple individuals separately, rather than relying on the sole verbal representations of one person. Finally, and most importantly, auditors should not rely only on evidence gained from interviews during audit planning or testing. They should obtain corroborating evidence by walking through transaction processes or by testing transactions using documented evidence.

Professional skepticism is vital to an internal auditor's mindset, whether he or she is gathering initial information to plan an audit or concluding on audit findings. Cognitive biases — such as truth bias, confirmation bias, and the halo effect — can compromise an internal auditor's professional skepticism. When this happens, it can lead to an overreliance on oral evidence, misinterpretation of answers received during audit interviews, and failed audits. Being aware of cognitive biases and the importance of professional skepticism can help internal auditors guard against these outcomes.

CHIH-CHEN LEE, PHD, CPA, CFE, *is a professor of accountancy at Northern Illinois University in DeKalb.*

MARK RILEY, PHD, CPA, *is dean and professor of accountancy at Northern Illinois University.*

REBECCA TOPPE SHORTRIDGE, PHD, *is chair in accountancy at Northern Illinois University.*

CLIFF NUXOLL, CIA, CFE, ACDA, *internal audit manager at Arthur J. Gallagher and Co. in Rolling Meadow, Ill., contributed to this article.*

TO COMMENT on this article, EMAIL the authors at chih-chen.lee@theiia.org

METAMORWORKS / SHUTTERSTOCK.COM

the RISKS in supply chains

Over the last couple of years, supply chain risk has become a key concern for the U.S. government. In December last year, for example, the U.S. Senate passed the Federal Acquisition Supply Chain Security Act of 2018, which contains powers to establish a security council specifically charged with supply chain risk. Further legislation with ramifications for supply chain management—such as the Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply Act—has been tabled at a federal level. The hazards are many, but all point to a recognition that with increasing globalization and digitalization, supply chains have become longer, less transparent, and open to a range of threats. That means a business anywhere in the chain with weak security and controls is a potential target.

"Supply chain risk is a huge issue in the U.S. right now," says Dan Shoemaker, director of the Master of Science in Information Assurance Program at the University of Detroit Mercy Center for Cyber Security and Intelligence Studies. He says it came to the attention of the U.S. government over fears that Chinese malware was turning up in U.S. military equipment. The risk with purchasing software is that vendors never give buyers the source code because of their need to protect intellectual property. So, companies effectively buy most software blind.

Shoemaker says this exposes organizations that build and use complex systems to two key risks: 1) malware can be injected into components at the bottom of the supply chain where transparency tends to be lowest; and 2) poor-quality counterfeit products can slip into a system because of cost-cutting pressures.

"This is the frontier in supply chain risk—we have systems built on top of systems that have all been built by mysterious people, and we have no idea who

A supply chain is only as strong as the business with the weakest controls.

Arthur Piper

TARAPATTA / SHUTTERSTOCK.COM

"Installing a standards-based process will help you understand what you are buying, because you can demand to see everything that is going on at any level of the supply chain."

Dan Shoemaker

"When the internal auditor does his or her job well, the cost recoveries are amazing."

Christopher Kelly

they are, and we often have no idea of how secure they are," Shoemaker says. He adds, half-jokingly, if he were a country that wanted to take over the world, he would set up shop as a cut-price programming shop. "Everything I sent up the process ladder would have a killer piece of software in it that basically said, 'When I push the button, I'll take over the world,'" he says. "That would be easy to do because unlike other things, we just buy software without carefully looking at the ingredients."

Internal auditors can suggest processes to reduce such supply chain risk, he says, and insist their organizations follow procedures established by the U.S. National Institute of Standards and Technology (NIST), such as NIST 800-161 that deals specifically with IT procurement and supply chain management, and also International Organization for Standardization (ISO) standards such as ISO 27000 dealing with information security.

"Installing a standards-based process will help you understand what you are buying, because you can demand to see everything that is going on at any level of the supply chain," he explains. "It will be documentation—not a physical examination of the actual activity—but that documentation will not be available otherwise."

COMPLEX CONTRACTS

In fact, supply chain documentation is often ignored or badly managed by the purchasing organization. Without a solid understanding of the contracts upon which agreements to buy are based, organizations run the risk of being arbitrarily overcharged by suppliers.

"Once signed, a shrewd supplier will hand the contract to their commercial department to start drafting claims against you while the ink is still wet," Christopher Kelly, partner at Kelly & Yang in Melbourne, Australia, says. Complex supply chains that entail huge, ongoing projects subject to multiple amendments can be daunting. But internal auditors typically can get to grips with the structure of their supply chains by mapping what it looks like. That will help flush out conflicts of interest between related-party companies, directors, and shareholders who may sit on both sides of a procurement deal, as well as reduce the risk of compounding overhead costs, for instance, within the project.

Contract agreements can be voluminous and take effort to digest, so internal auditors who put in the hours have a fighting chance of helping their organizations manage them because each contract effectively builds its own distinctive rules around costs, profits, and target parameters, Kelly says. Failing to understand the contractual intricacies is the No. 1 mistake internal auditors make, he adds. Internal auditors trained in financial accounting, for instance, cannot assume that they will be able to apply Generally Accepted Accounting Principles to any items of expenditure. IT costs allowable under the contract as a direct cost, for example, may already be included in the overhead rate. Accruals may or may not be allowed. Only the contract's terms will make the correct treatments clear.

If the organization and its internal auditors are on top of their contracts, however, data mining and analytics become a powerful way of validating the costs charged against those allowed under the contract. That requires attention to detail. Keyword searches for entertainment, gifts, parties, or rework because of the supplier's mistakes can expose multiple errors, duplications, and advance charges, for instance. Cost analysis also reduces the risk of organizations being charged up front by the supplier for work not yet completed and then the supplier going out of business.

56% of health-care organizations have experienced a **data breach** introduced by one or more third-party vendors in the last two years, according to research from Censinet and the Ponemon Institute.

2019 SUPPLY CHAIN TRENDS

The five themes impacting supply chains most in 2019:

- » Revision of the Minimum Security Criteria under the U.S. Border Protection's Customs-Trade Partnership Against Terrorism (CTPAT).
- » Supply chain growth in Africa, which increases exposure to risks.
- » Ongoing mass migration, which poses both security and corporate social responsibility risks.
- » Dramatic shifts in politics, such as elections in Brazil, the U.S.-China trade dispute, and uncertainty over Great Britain's departure from the European Union.
- » The continued threat to supply chains posed by cybersecurity issues.

Source: BSI's Supply Chain Risk Insights 2019 report.

"When the internal auditor does his or her job well, the cost recoveries are amazing," Kelly says. The biggest recovery he achieved was about $9 million. "I didn't get a bonus, but it got me noticed," he says. "And as an auditor wanting to advance in his or her career, that's not a bad thing."

Outside of the contract terms, changing the manager on the buyer side of the contract can be disastrous. On one audit, Kelly found that while the supplier had used the same manager on the project for 10 years, there were frequent changes to management personnel at the buying business. "The contractor was running rings around the buyer with unbudgeted charges, and when I asked for the contract, I was shown a heap of boxes and told, 'We think it's in there,'" he recalls. "It's vital to keep continuity of knowledge when managing large-scale projects."

BUILDING RESILIENCE

New supply chain risks are not as easy to detect and deal with. "We're seeing key shifts to global supply chains this year, driven by quite dramatic changes in the geopolitical landscape," said Jim Yarbrough, global intelligence program manager at BSI, the business standards company, at the launch of a new report this year (see "2019 Supply Chain Trends" on this page). "The concern is that as supply chains change — with Chinese companies moving operations to Africa, for example, or the U.S. sourcing goods from other Southeast Asian nations — major implications will also evolve."

Rapid change requires a flexible strategy from internal audit teams. "It is important to look at the sup- ply chain through the lens of risk and resilience," Jonathan Eaton, practice leader in Grant Thornton's National Supply Chain Practice in Charlotte, N.C., says. "That means digging into the operating model to identify the potential failure points."

Internal auditors can do that by using a Six Sigma tool called failure mode and effects analysis (FMEA), for instance, or a host of other tools.

> The supply chain should be looked at through the lens of risk and resilience.

But, he says, the question they need to address is, "In your unique business model and industry, what are the failure modes within your supply chain that can hurt your business?" Eaton says that's something audit leadership will ultimately need to determine. "The buck stops with the chief internal audit executive on this," he says. "If he or she knows that a business could

"If people want to evade sanctions, they will lie—which is where sanction risk crosses over into potential fraud."

Samar Pratt

"The people who manage the supply chain have to be forthright with internal audit about what the risks are and the triggers that make them real."

Jonathan Eaton

be vulnerable within the supply chain, but does not know where, when, or why, then he or she must take action to find out. A deep dive into the processes using FMEA is a great place to start."

Internal audit leaders need to ensure they are positioned as a trusted advisor to the business; otherwise, helping the business deal with supply chain risk is going to be virtually impossible.

"You have to be able to proactively track, manage, and measure risk," he says. "But nobody has a silver bullet that is going to deal with all of the possible combinations of risk that can arise. That is why having a good relationship with the business is important for internal auditors, because the people who manage the supply chain have to be forthright with internal audit about what the risks are and the triggers that make them real."

This task recently has become more difficult. Many companies have expanded their business and sales through the use of multiple sales channels, and they often have not reconfigured their supply chains to deal with the range of new platforms or delivery requirements that are in play. Managing risk in the supply chain in this scenario becomes a way of protecting against the potential erosion of profitability, says Eaton, and internal audit needs to have an in-depth knowledge of the business' operations to be able to truly assist the organization in this area.

He sees the ability to track, manage, and measure risk as internal audit's central role when it comes to supply chain resilience—particularly because those processes should be aligned to the biggest financial supply chain risks the business faces. Eaton describes robotic process automation (RPA) as a brilliant tool once audit understands the business' failure modes and its strategy for tracking, managing, and measuring risk. RPA deals with high-volume, repetitive processes, so it can continually scan supply chain transactions in real time and be programmed to alert for weaknesses and red-flag events. He says too few businesses have made this move. "Internal auditors can introduce thought leadership into an organization in this area by bringing in these advanced technologies to mitigate the risk and build supply chain resilience," he adds. But he also warns that an overdependence on technology and analytics can equally make internal audit blind to the more complex interrelated risks in the supply chain. For supply chain technology to work well, it needs to be aligned strategically with the business' objectives for supply chain risk management.

PREVENTING CRIME

Supply chains are also open to bribery, corruption, money laundering, and human trafficking risks. More recently, sanctions have become a pressing issue as the trade war between China and the U.S. gathers pace, and the Trump Administration applies pressure on its allies to keep its sanctions against Iran effective, for instance. The Office of Foreign Assets Control, the U.S. sanctions watchdog of the Department of the Treasury, has been increasing its activity in this area.

"Corporations need to make sure they understand the risk in their supply chain if they want to avoid being caught in the crosshairs," says Samar Pratt, managing director of Exiger, a global governance, risk, and compliance business in London. But she warns that the boundaries between different types of risks can be porous. "If people want to evade sanctions, they will lie—which is where sanction risk crosses over into potential fraud," she says.

Internal auditors should expect their organizations to do solid due diligence checks, she says. "While there is only so much a firm can do, as long as

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

it can demonstrate it is taking a risk-based approach to its due diligence, it will help the organization demonstrate to internal audit it is taking appropriate steps. As part of this process, organizations are increasingly using artificial intelligence-powered, automated due diligence technology to detect red flags while onboarding new suppliers, or to monitor third parties on an ongoing basis." Other methods include looking at the countries where raw materials are coming from, for instance, and, potentially, where the risk warrants it, sending people to those countries to ask questions on the ground.

"The due diligence needs to be proportionate to the risk and reflect the risk appetite of the organization," she adds. While internal auditors are not specialists in investigating fraud in the supply chain, IIA standards require them to look for fraud indicators. If found, internal audit is likely to refer those issues to the organization's fraud or financial crime team and possibly the legal team. Pratt says internal audit's follow-up role is frequently overlooked. That involves coming back in post-investigation to examine what went wrong in the supply chain and add significant value to the business by focusing on the lessons learned and whether controls need to be strengthened.

MAKING AN IMPACT

While the direct impact of mishandling a contract or breaking a government sanction can be significant, the reputational damage can be equally long-lasting and harmful. And as geopolitical risk increases and digitalization gathers speed, supply chain resilience is likely to become even more important. It is a difficult area for internal auditors to master. Doing so requires wide-ranging knowledge of different types of contracts, the business, and its supply chain structure—as well as keeping up to date with fast-changing threats. But the rewards can be great. Internal auditors who can play a central role in helping their organizations build robust supply chains will enable them to compete globally and successfully integrate new products and services into their offerings.

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

Internal auditors should examine several "tacit truths" that often hinder organizational ethics.

6 Myths of Business Ethics

Matej Drašček

Recent corporate scandals at companies such as Nike, Volkswagen, and Wells Fargo have spotlighted the negative impact of poor ethical cultures. Meanwhile, public trust in business and government is low.

Ethics is a key part of corporate governance. The past three decades have seen several moves to improve business governance and ethics: The Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control–Integrated Framework*, the U.S. Sentencing Reform Act, and the U.S. Sarbanes-Oxley Act of 2002 and similar legislation in other countries.

Ethics is a cornerstone of internal auditing, as well, both in terms of the ethics of practitioners and the profession's role in providing assurance of organizations' ethical practices. The *International Standards for the Professional Practice of Internal Auditing* Standard 2110: Governance calls on the internal audit function to assess the organization's ethical climate, and The IIA's Practice Guide on Evaluating Ethics-related Programs and Activities describes procedures to help auditors review organizational ethics.

Yet, in addressing ethics, organizations and internal audit often are hindered by several myths. Internal auditors should step back and assess whether these "tacit truths" about ethics are actually helping organizations become more ethical.

DAVOODA / SHUTTERSTOCK.COM

Myth 1 The Code of Conduct Supports Ethical Behavior

The first step in planning an audit of ethics is to check whether the organization has a code of ethics or conduct designed to help the organization and its stakeholders behave ethically. In fact, most publicly traded companies around the world are legally required to have a code in place.

However, the main risk is not whether the code of conduct exists, but how it is used in the organization. There is mixed evidence that conduct codes actually help improve the ethical climate. Implementing a code of conduct could reduce ethical behavior, according to a 2011 study published in *Decision Sciences Journal*. A 2005 Harvard Business School study shows that the main goal of such codes is not to improve an organization's ethical climate but to reduce possible legal fines in case of prosecution. Moreover, a 2018 *Harvard Business Review* study conducted by Hui Chen and Eugene Soltes found that a code of ethics has no impact on ethical decision-making.

How to address this myth Internal auditors should examine the actual practices of their organization's code of conduct. Employees annually signing the code, checking for specific compliance policies in place to support and provide additional guidance on key components of the code, and conducting focus groups or surveys to assess the code of conduct are not enough. Based on various behavior experiments, the best practice is to require decision-makers to read and sign a statement that they are complying with the code before making every major decision, according to the book *The Honest Truth About Dishonesty* by Dan Ariely.

Myth 2 The Compliance Program Helps the Organization Become More Ethical

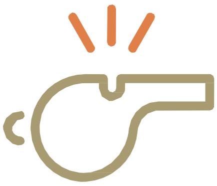
The average multinational company spends several million dollars a year on compliance, which can be even greater in highly regulated industries such as finance and defense, according to the 2018 *Harvard Business Review* article by Chen and Soltes. Despite such spending, executives complain that compliance does not offer any tangible ethical benefits. Putting these two trends together, executives are struggling to see how compliance can help improve ethics in the organization.

Compliance programs are caught in the same dilemma as ethics codes: The primary goal is to satisfy regulatory requirements or reduce penalties, rather than actually help the organization become more ethical. Internal auditors also should keep in mind that compliance issues are not the same as ethical issues — what is legal is not the same as what is ethical and vice versa.

How to address this myth For compliance programs to have a meaningful impact, internal auditors need to test what works and what doesn't. The compliance program should experiment and innovate. One way is to test assumptions about how people actually behave versus what they say they do. Compliance should test which programs or internal controls work — using hypothesis testing or control and testing groups — to see why people do not follow the rules and how rules should be presented to them. For example, some people respond more to visual information, so for them, rules should be presented in a different form than for those who respond more to audio.

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

Myth 3 Whistleblowing Tools Reduce the Risks of Unethical Behavior

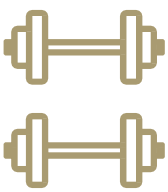


The recent case of Nike, which faces gender discrimination lawsuits despite taking steps to alter its culture, shows that sometimes, even if the tools of enhancing ethics in an organization are enforced and communicated, unethical behavior may persist. EY's 14th Global Fraud Survey finds that people do not want to report wrongdoing and that reporting comes with significant risk. Challenging the status quo in any organization threatens people's status and relationships with their supervisors and colleagues. Moreover, whistleblowing can be a self-serving tool when combined with the bystander effect—when a person is in trouble, others who are present often fail to intervene because they assume other people will do so or because they think it's not their place to act.

How to address this myth The objective of whistleblowing should be to detect wrongdoing more timely. There are several ways whistleblowing can achieve this goal:

- Establish legal protection for whistleblowing at the national, industry, organizational, and labor contract levels.
- Offer financial benefits to whistleblowers.
- Test whether the hotline works and is confidential—for example, by using "mystery tester" reports.
- Conduct a mock performance of unethical behavior, such as deliberately backdating and signing a document in front of employees or staging an act of employee harassment, to test whether anyone reports it.

Myth 4 More Training in Ethics Is Better



The common way to measure ethical training programs is with completion rates, which are normally between 90% and 95%, according to Deloitte and *Compliance Week's* 2016 Compliance Trends Survey. The problem is that this metric shows neither the quality of the training nor its effectiveness. Research by Carmel Herington and Scott Weaven shows that more training in ethics is not better and can sometimes reduce the engagement of employees. However, training programs are easy to measure, and managers therefore encourage using them.

How to address this myth The organization should strive for the quality or customization of training for each employee. Ethical behavior is not something that is the result of policies but is a practice that, as Aristotle says, becomes part of the person when in use. Organizations should tailor ethics programs to the individual's specific need, moral development, and character. At the very least, customization should be based on functions and corporate hierarchy, followed by measurement of employees' moral development, with subsequent training sessions grouped based on the results. Ideally, training should be conducted in person rather than online and use real examples from people and organizations—especially ethical dilemmas that do not have an easy fix.

Myth 5 Individual Unethical Character Can Be Curbed With the Right Internal Controls

One outcome of the 2008 financial crisis is that it provided evidence that the character of executives was a contributing factor to the worldwide crisis. For auditors, it should be clear that personality and character are not the same. The main difference is that personality may change over time, but character remains the same.

IMAGES: TOP, PICONSME / SHUTTERSTOCK.COM; FAR LEFT, HN WORKS/ SHUTTERSTOCK.COM; LEFT, ALEXANDR III / SHUTTERSTOCK.COM

Favorable ethics outcomes rise **11 fold** when employees are **encouraged** to base decisions on organizational values and standards, according to ECI's 2018 Global Business Ethics Survey.

Also, personality is the range of distinctive personal qualities and traits of an individual, but character refers to a set of morals and beliefs that defines how the individual treats others or behaves with others and himself. Changing character is not possible, though organizations are spending millions of dollars on these kinds of programs.

How to address this myth When an employee is already in the organization, it is fruitless to try to change his or her character to become more ethical. The root cause lies in the hiring process. Human resources practices are normally good at testing or examining the technical competencies of candidates as well as evaluating personal traits. When it comes to testing the ethical character of the candidates, most organizations fall flat. Internal auditors should check whether the organization's hiring practices examine job candidates' moral development. One well-established test is the Heinz dilemma, a thought experiment developed by psychologist Lawrence Kohlberg to assess moral reasoning skills, which ranks participants along six stages ranging from obedience to universal ethical principles.

Myth 6 Goals Related to Ethics or Compliance Help Organizations and Individuals Behave More Ethically

When Enron went bankrupt, both independent investigators and company officials were clear: Enron's goal-setting practices, which involved setting difficult and specific performance goals for employees, were at the heart of the misconduct. In fact, many of the goals were connected directly to compliance and ethics, such as ethics training completion rates and regulatory fines paid. Moreover, a growing body of academic research demonstrates that giving people specific, challenging performance goals can cause them to cheat on tasks or misrepresent their performance. In addition, pressures that companies face striving for quarterly earnings targets or personal goals in employees' annual appraisal interviews can contribute to unethical behaviors.

How to address this myth If goals can lead to unethical behavior, following the organization's purpose can help build ethical behavior, according to *Nine Lies About Work* by Marcus Buckingham and Ashley Goodall. When the organization has a purpose beyond maximizing value or profit, employees develop a sense of belonging and behave more ethically no matter the specified goals. Moreover, strides in ethical behavior result from practice and repetition, which should be integral to the organization's approach.

Reflective thinking can help with this process. Reflective thinking is the critical-thinking process that refers specifically to analyzing and making judgments about what has happened. Reading clubs that feature books that deal with ethical issues, regular meetings about ethical decision-making, and ethics "hackathons"—exercises that examine the ethical implications of a particular technology—are some methods to foster reflective thinking in the organization.

ALEXANDR III / SHUTTERSTOCK.COM

BEING COURAGEOUS

In letting go of these well-intentioned but misguided myths about ethics, internal auditors should use critical thinking to challenge principles or practices that seem to be great at first, but actually could only be fads. The foundations of critical thinking are Socratic questioning of evidence, closely examining reasoning and assumptions, analyzing basic concepts, and tracing implications both of what is said and of what is done. Especially where business ethics has challenges and old ways of doing things that do not work anymore, critical thinking becomes essential.

Courage is another integral part of auditing ethics. To speak up and show where the ethical risks lie sometimes involves going beyond the limits of the organization. Internal auditors should have the courage to go further and not be afraid.

Ethics is a struggle against human nature. New threats lie everywhere, and sometimes people test the boundaries. It is the auditor's role to gather his or her courage and say "no" to these temptations, and to believe that sometimes it takes just one individual to change the way people and organizations behave.

MATEJ DRAŠČEK, CIA, CRMA, *is chief audit officer at LON Bank d.d., based in Domžale, Slovenia.*

Social Media

Social media's strategic role within organizations has grown exponentially as it has become a ubiquitous juggernaut of nonstop information of varying degrees of accuracy and relevance. But its risks to the organization have accelerated, as well. To keep up, organizations need a strong governance structure that specifically emphasizes social media.

Similarly, social media's high impact [illegible]ean internal audit should look closely at all related activities. Perhaps the most important of these activities for internal audit is ensuring the organization's social media governance is effective.

IT STARTS AT THE TOP

Any aspect of governance starts with the board. As part of its assurance efforts, internal audit should ensure the board understands the broad scope of risks related to social media, as well as the board's role in establishing an appropriate governance structure.

Foundationally, the organization already should have an effective governance structure in place. But the fast pace of change related to social media means the board should take a more active role in ensuring the organization's governance structure addresses unique social media issues effectively. This not only helps the organization successfully achieve these objectives, but also further ensures the organization will not be broadsided by change, irrelevance, and damaging reputation issues.

The board must understand the changing landscape of social media, as well as the current and evolving risks. Further, directors must understand the organization's social media strategies — both the strategies specific to social media and those using social media to better achieve objectives. This includes understanding how the strategies were developed and how they support the organization's overall mission. Finally, the board should understand how the organization will address emerging issues, potential crises, and the overall changes in the social media environment.

Ultimately, board members must be able to lead conversations that get to the heart of the organization's approach (see "Questions the Board Should Ask" on page 55). To ensure the board is prepared to successfully oversee social media activities, internal audit should focus on three areas: knowledge, training, and communication.

Knowledge The constant press coverage related to social media "fails" has resulted in boards becoming more aware of social media's risks and pitfalls. But it also has led many boards to focus on the latest YouTube debacle or Twitter mistake, rather than understanding the broader risks. Therefore, internal audit should ensure board members fully understand the risks and opportunities related to social media, as well as the organization's activities.

Training Internal audit should ensure the board has been trained appropriately on new and emerging social media technologies, how they are used, the risks to the organization and its industry, and how competitors are using social media. Such training will help the board understand how the organization developed its strategic approach and what it needs to be successful.

Communication Internal audit should ensure communication channels allow the board unfettered and timely access to the information it needs about social media. In addition to information from executives, this communication should come from committees responsible for social media, departments involved in developing and communicating through social media, and front-line personnel who are dealing with day-to-day issues that can quickly grow into organizational disasters.

Internal audit can provide assurance that board members are prepared by examining activities at the highest levels of the organization. The best way is for auditors to speak directly with board members to gain assurance that directors are providing the best oversight possible. Additionally, auditors should review correspondence and minutes of board meetings, as well as the information received by the board, to ensure that it has been kept in the loop. They also should review training materials to ensure materials cover all appropriate areas and that all board members have participated.

EXECUTIVE OVERSIGHT

At the next layer of governance, the executive level is responsible for developing and implementing the organization's social media strategies and objectives, as well as ensuring they align with the organization's other strategies and objectives. Like the board, executives should obtain assurance that social media projects are advancing as expected, the projects are aligned with other strategies, the objectives are being met, significant risks and issues are communicated, and all other necessary information is brought to executives' attention timely.

Best practice is to assign a social media champion at the executive level to oversee social media activities organizationwide and be responsible for their success. The executive should fully understand and believe in the value of social media to the organization, while also understanding the associated risks. This individual also should have the status to freely communicate potential issues and concerns to fellow executives. Otherwise, social media activities may fail because of lack of interest.

It also is best practice to establish a social media oversight committee to handle responsibilities at a more granular level. The committee should encompass all departments with a role in social media and include individuals with the authority to initiate changes. The committee will be responsible for ensuring the alignment and success of all social media strategies, objectives, and plans; monitoring project progress; and communicating potential issues. The executive

Governance

Internal audit can make an impact by looking at how the board, executives, and three lines of defense address social initiatives.

J. Michael Jacka and Peter R. Scott

SERGEY NIVENS / SHUTTERSTOCK.COM

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

champion should be an active member of this committee, providing guidance and ensuring necessary communication between the committee and executives.

Much of internal audit's review of executive oversight is similar to that outlined for the board—just more detailed. This includes obtaining assurance that executives receive ongoing training that allows them to understand how social media can best be used, and that executives are adequately updated on social media. In addition, internal audit should determine whether executives are actively ensuring their individual departments are using social media appropriately, and that those activities are aligned with other departments and functions.

Interviews with executives are the best way for auditors to obtain this information. And, while social media-focused interviews can be an important part of the review, an effective alternative is to discuss the topic in meetings about departmental risks, concerns, and upcoming initiatives. Special attention should be paid to the executive champion, who can be a significant source of information about the status and growth of social media. If the relationship is cultivated appropriately, the champion can be a source for potential areas of review.

> **The executive champion can be a significant source of information about the status and growth of social media.**

THE FIRST LINE OF DEFENSE

A challenge in any governance structure is ensuring coordination among the teams that manage the various aspects of risk. Effective social media governance requires each of the three lines of defense—operational management, risk management and compliance functions, and internal audit—to understand the specific risks and responses that apply to their functions.

The first of these lines, operational management, owns and manages the risk. These are the operational managers responsible for maintaining effective internal controls and executing ongoing risk and control procedures. Each operational function must understand the impact of social media on its responsibilities, as well as the function's role in the organization's social media presence. Although their roles and responsibilities can vary from one organization to the next, the following are functions that could be involved with social media.

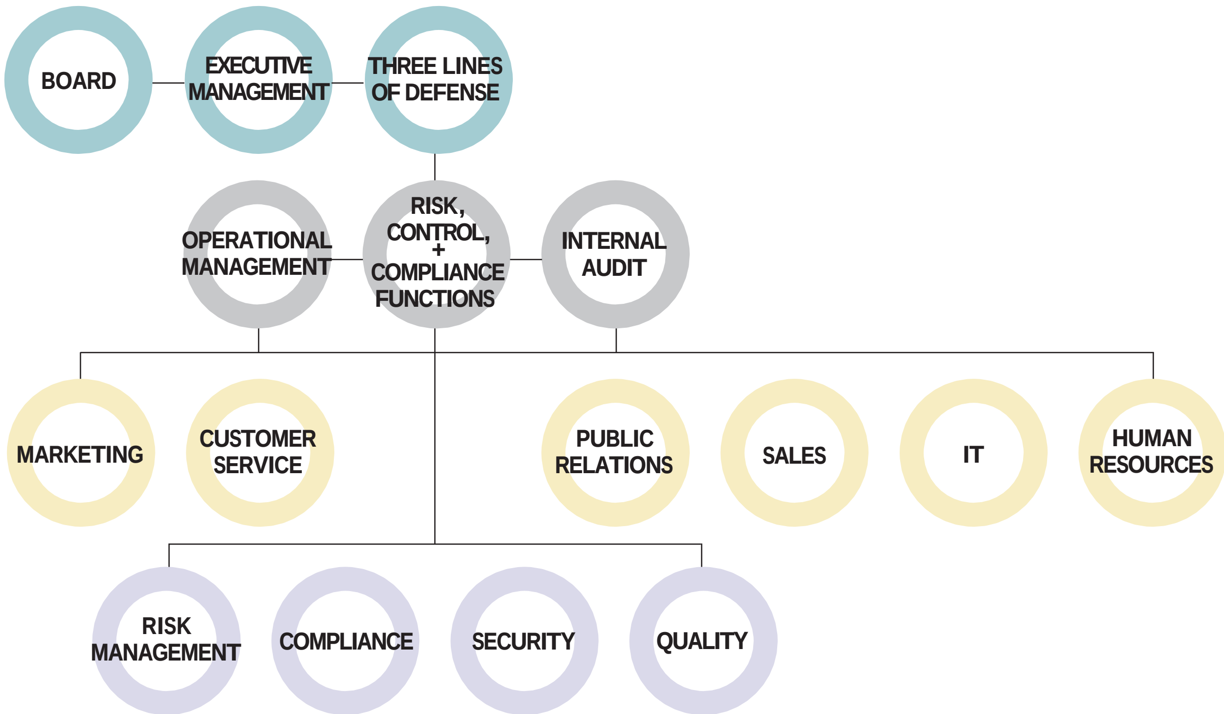
Marketing This function is responsible for marketing through social media channels, including brand management. Responsibilities include ensuring social media delivers a consistent message to the right customers, brand integrity and standards are maintained in all social media channels—including the activities of agencies and third-party ven- dors—and the message being delivered matches organizational objectives.

Sales The sales function's responsibilities include ensuring sales efforts on social media match marketing's message, delivery of products and services sold through social media is accurate and timely, and follow-up is taken on leads generated through social media. The department also must keep online sales information updated and accurate, and use social media data to analyze trends related to leads, sales, and returns. Ultimately, the function should ensure social media improves sales efficiencies and costs.

Customer Service This function ensures complaints received through social media are handled efficiently, customer satisfaction in the online sales process is maintained at the desired

59% of companies say social media is very important to their marketing strategy, but just 30% say it has been very effective, according to Buffer's State of Social Report 2019.

SOCIAL MEDIA GOVERNANCE AT A GLANCE



levels, and customers are referred to the appropriate goods and services. Customer service also makes sure all online communications maintain the appropriate tone and social media is used to accurately measure customer satisfaction.

Public Relations Also known as corporate communications or community relations, public relations manages how the public perceives the organization. Its responsibilities include ensuring social media messages related to public relations match the overall messaging strategy and monitoring exists to identify, avert, and mitigate crisis situations. Public relations also should have an effective crisis management plan that includes responding to social media issues and using social media as part of the crisis management process.

IT This function develops and maintains hardware and software used for social media. IT's responsibilities include ensuring customers have a seamless experience while using social media and maintaining sufficient backups to reduce or eliminate downtimes. This function implements technology to achieve the organization's social media objectives and ensures access to the organization's social media sites is controlled.

Human Resources This function uses social media to recruit new employees and potentially uses social media to deliver training. Human resources should ensure that training on the use of social media includes all employees and all facets of social media use. It should ensure a social media policy is developed that complies with existing regulations and the organization's other policies, and monitor employee satisfaction through external comment boards and websites.

THE SECOND LINE

The second line of defense comprises those functions that ensure first line of defense controls are designed appropriately, in place, and operating as intended. Spanning the organization, these functions provide assurance related to their field of expertise. Second line functions need to keep abreast of changes in social media with a particular emphasis on issues impacting the areas they oversee. As with the first line of defense, the specific structure and responsibilities of second-line functions differs among organizations. In reviewing governance, internal audit should ensure that the organization is addressing all of the potential social media oversight roles these functions perform.

Risk Management This function ensures social media risks are understood throughout the organization and included in risk assessment processes. Responsibilities include ensuring all risk assessments consider social media, departments keep abreast of emerging issues and risks related to social media, and those issues and risks are communicated timely. The risk function also must ensure all departments' risk assessment and management procedures address social media risks appropriately.

Auditors should consider providing an overview of organizationwide responses to social media risks.

Compliance The compliance function is responsible for ensuring existing regulations are reviewed for reinterpretations that may impact social media and that new and changing regulations are monitored. It must advise all departments of regulations that will impact their use of social media and ensure that potential noncompliance issues are reported and acted upon.

Security The security function must ensure appropriate access to and control over social media activities. It ensures general IT security controls such as password, antivirus, anti-malware, and firewalls have been established and are being used effectively. It also makes sure that access to the organization's social media accounts is restricted appropriately, all accounts are monitored for suspicious activity, and accounts that are no longer in use have been decommissioned. Additionally, the security function should ensure all employees understand the risks related to inappropriate use of social media.

Quality This function is responsible for ensuring the organization's use of social media complies with standards related to brand and image. Its responsibilities include ensuring branding and imaging within social media accounts match established standards, and making sure overall quality and professionalism of social media interactions match the desired level. The quality function also should ensure information reported through social media channels is accurate, and the organization takes effective corrective action on identified issues.

THE THIRD LINE

Internal audit provides the board and senior management with independent and objective assurance of the other two lines' efficiency and effectiveness. To that end, auditors should ensure that all entities in the three lines understand social media risks as well as their responsibilities for those risks. Internal audit can use two approaches to provide this assurance.

The first is to conduct an overall review of social media, focusing on the functions where the greatest risk may reside. This review may entail separate audits of social media for each function—which will provide detail on how the function is performing—or a review of social media risks, adding focus on potential gaps among departments.

The second approach is to include social media as a risk area in all audits planned for the year. The results should be included in the individual reports, but auditors also should consider providing an overview of organizationwide responses to social media risks.

AUDIT'S SOCIAL IMPACT

Social media has become an integral part of any organization's success and an area that internal audit functions ignore

71% of consumers who have a positive social media experience with a brand are likely to recommend that brand to their family and friends, Lyfe Marketing reports.

QUESTIONS THE BOARD SHOULD ASK

A well-informed board is equipped to ask the important questions about the organization's use of social media. To ensure the organization understands its social media strategies and direction, here are some questions board members should be prepared to ask and the organization should be able to answer.

How are we using social media to engage with our customers, open new markets, and recruit top talent?
These three areas are only a small part of how the organization is using social media. But they provide a good foundation to ensure the organization understands the impact of social media, and they may help the organization explore how best to use it.

How are our competitors using social media?
Social media is a competitive advantage. Without understanding how the competition is involved, the organization cannot know if it is ahead of or behind the curve. Understanding the competition's use of social media also provides lessons learned without actually taking the risks. In addition, following competitors on social media provides insights into their strategies and plans beyond social media.

How are our employees and other stakeholders using social media? What do we allow?
This question generally will lead to a discussion about existing social media policies. But the primary purpose is to provide assurance that the organization is aware of the risks related to employee and stakeholder use of social media, is monitoring those activities, and is prepared to respond quickly to potential issues.

What regulations regarding social media does our organization need to be aware of?
Board members need assurance that the organization understands the impact of regulators on the organization's use of social media, monitors compliance with those regulations and regulatory changes, and takes appropriate actions.

How are we monitoring social media activity for potential negative issues? Does this include plaintiff, activist, regulator, and vendor social media activity?
Monitoring is an important part of the organization's social media risk management process. Almost every social media fail could have been better controlled had the organization monitored and responded to social media conversations appropriately. Monitoring can provide early warning about public relations, brand, regulatory, or legal issues before they get out of hand.

How are we interacting with the organization's followers, friends, etc.?
The board needs to understand how success is measured related to the investment in social media. The important aspect of this question relates to how any measures of success will be used to positively impact organizational objectives. Board members should be asking for a direct link between social media metrics and broader organizational success.

What do board members need to do to ensure they keep out of trouble?
First, the board must be assured that it has the information necessary to understand and respond to relevant social media risks. Second, board members must understand how their use of social media—whether as a representative of the organization or as a private citizen—can impact the organization. While these are questions that should be asked by board members, they also are excellent questions for internal audit to use during its reviews, particularly at a governance level. The questions dig deeply into the knowledge and awareness of all social media participants.

Adapted from "Critical Social Media Questions for the Board Room" by Richard S. Levick, Fast Company, *11/27/12.*

at their own peril. In providing assurance regarding social media, governance can be one of the most impactful areas in which internal audit can provide value. Moreover, reviewing governance establishes a foundation upon which internal audit can begin to build its understanding of, and assurance work related to, social media. Ia

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

PETER R. SCOTT, CAE, APR, *is CEO at the American Academy of Optometry in Orlando, Fla.*

Jacka and Scott are the authors of Auditing Social Media, *Second Edition, published in August by The IIA's Internal Audit Foundation.*

Board Perspectives

BY JIM PELLETIER

BLUE BELL BLUES

Growing case law affirms board liability.

Investor lawsuits seeking to hold directors liable for failures in their oversight duties were bolstered in June by a case involving Blue Bell Creameries. *Marchand v. Barnhill* did not signal a change in law, but it did affirm a legal standard that boards that fail to make a good faith effort to oversee a material risk area breach their "duty of loyalty."

Legalese aside, the Blue Bell case provides a compelling example for directors to examine. While legal standards set a high bar, *Marchand* demonstrates that, in certain circumstances, ignorance about poor risk management is not a defense against board liability.

The details around the lawsuit are well-established. A 2015 listeria outbreak linked to three deaths caused Blue Bell Creameries to shut down production, recall all products, and later reduce its workforce by more than one-third. An investor suit alleged senior management disregarded warnings about contamination risks and kept the board in the dark about the issue.

From 2009 through 2014, regulators identified numerous health safety compliance failures. Yet, even though several positive tests showed the presence of listeria, including one test from an independent lab, board minutes reflected "no board-level discussion of listeria."

Despite what would appear to be a glaring lack of board oversight, the Delaware Court of Chancery dismissed the case in fall 2018, ruling the plaintiff failed to show that directors had breached their "Caremark duties."

What Are Caremark Duties?

Caremark duties are the result of a 1996 Delaware Chancery Court decision in the derivative action case brought by shareholders of Caremark International Inc., alleging the board of directors breached its duty of care by failing to put in place adequate internal control systems. The Caremark Rule that came from the case, and set a precedent for future director liability claims, states, "a director's obligations includes a duty to attempt in good faith to assure that a corporate compliance information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."

Cutting through the legalese again, Caremark establishes an obligation for directors to at least try to make sure "a reasonable board-level system of monitoring and compliance" is in place. Failing to do so could make directors liable for losses relating to compliance failures.

In *Marchand*, the Delaware Supreme Court

READ MORE ON STAKEHOLDER RELATIONS visit InternalAuditor.org

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

overturned the lower court's dismissal, concluding "the complaint supports an inference that no system of board level compliance monitoring and reporting existed at Blue Bell." The court noted the board failed to establish a committee to monitor food safety or devote time in meetings to discuss food safety compliance. Of significance is the court's opinion that "... food safety was essential and mission critical."

Protecting Against Caremark Failures

Reasonable and informed directors typically should not have to worry about Caremark failures. As the Delaware Supreme Court made clear, boards get into trouble when they ignore their oversight responsibilities.

There are valuable lessons in the court's findings in *Marchand* that can help protect boards and head off behaviors that make them vulnerable to successful Caremark claims. It is important to note that the court's findings that follow cen- ter on the Blue Bell board's failure to understand its "mission-critical" risk: food safety.

Blue Bell had no board committee that addressed food safety. Boards must understand what is mission critical for their organization, whether it's food safety at Blue Bell or data protection at Facebook, and assure that it has systems in place to monitor compliance with mission-critical regulations.

Blue Bell management was not required to keep the board informed about food safety compliance practices. Boards cannot assume management will bring all problems to their attention, and, therefore, must be proactive in seeking out information about compliance with mission-critical risks.

Blue Bell had no regularly scheduled discussions about food safety. Mission-critical risks must be discussed and assessed on a routine basis by the board.

Blue Bell's board received favorable information about food safety but negative information was not shared. Boards cannot assume that management will willingly present the bad along with the good. It must establish processes to discover all relevant information from management and seek additional reliable sources of information, including turning to internal audit to provide independent assurance on the accuracy, completeness, and timeliness of the information the board receives, particularly around mission-critical risks.

Blue Bell board minutes reflect meetings were "devoid of any suggestion that there was any regular discussion of food safety issues." Traditional approaches to protecting the board include limiting details in minutes, which often only reflect official board actions. In Blue Bell's case, this strategy backfired in that the official account of business reflected that no time was spent discussing mission-critical issues.

What's Next?

The *Marchand* case and its relevant Caremark implications are but one of a growing number of pressure points on boards relating to oversight duties. As the list of governance failures and scandals grows, regulators, investors, and the general public are demanding more oversight and more accountability.

A February article in *Business Law Today* eloquently articulates the need for a fundamental change in how board directors approach their jobs:

> "A substantive checks and balances approach addresses the roles, responsibilities, and relationships among the key elements and players in a firm's governance, controls, and oversight system. Institutional investors, individual investors, and other market and regulatory interests increasingly demand that those involved in corporate governance recognize their responsibilities and are held accountable in addressing these responsibilities. An additional emerging expectation is that senior leaders in an organization, both board and management, recognize that a leader's role is one of service rather than entitlement."

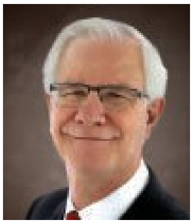
The article goes on to say that governing structures that consolidate power and authority into fewer hands often fail if individuals in power feel entitled to do as they please. It adds that boards must be involved in formulating checks and balances and take active roles in executing them. "Carrying out these active roles will necessarily lead to regular interaction with the CEO and others in senior management as well as with a company's internal and external auditors," the authors write. "While tone at the top may sometimes remain only as words that do not actually affect behavior, the institution of checks and balances can exert considerable influence."

These fundamental changes won't happen overnight, especially in organizations with entrenched systems and practices. But clearly the era of boards providing obsequious approval to management is over. To continue to do so is not just counter to prevailing investor sentiment, it also makes boards increasingly susceptible, as demonstrated in *Marchand*.

Such a transition cannot happen without a system of effective checks and balances, as described in the *Business Law Today* article. Given this current environment of increased exposure, boards would do well to seek internal audit's independent assurance and advice on critical issues. Ia

JIM PELLETIER, CIA, *is vice president, Standards and Professional Knowledge, at The IIA in Lake Mary, Fla.*

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



BY J. MICHAEL JACKA

DON'T JUST MEASURE IT, DO SOMETHING!

Auditors should make sure they're measuring the right things—and using results the right way.

How do you measure the success of your internal audit department? The subject comes up repeatedly in conferences, articles, research, and chapter meetings. It is obviously an issue that plagues and perplexes audit departments everywhere, and finding the answer seems to be a holy grail quest for the profession.

The challenge certainly doesn't come from a lack of possibilities. Everything from audits completed to use of available audit hours to requests for audits to customer satisfaction to corrective actions completed to efficiency improvements identified to certifications achieved to the number of auditors who can dance on the head of a pin have been suggested, adopted, and rejected. But we all continue to search for internal audit's success-measurement El Dorado.

The reason our search continues to fail, even with this unending supply of possibilities, is that audit departments forget two important rules pertaining to the development of success measures. Rule No. 1: The measures should be developed in support of the audit department's mission. If the department cannot demonstrate how the measures support that mission, then they become vanity measures serving no purpose other than saying, "Look at us!" Note also the assumptions built into this rule—internal audit has a mission statement, that mission is in alignment with the organization's mission, and every auditor knows and can recite the mission statement. Missing any of these elements results in ineffective measures.

However, most important is rule No. 2: At the end of the day, have a plan for how all those measures will be used. Author and marketing guru Seth Godin once stated, "Don't measure anything unless the data helps you make a better decision or change your actions." And unless an audit department uses its measures to improve internal audit's choices, do better work, or make the department more effective, then collecting the associated data is just a waste of resources, time, and effort.

Many audit functions measure, but I have seen very few that use those measures to get better. At most, if they are not meeting the criteria promised to the audit committee, there will be much wailing and gnashing of teeth as the chief audit executive promises improvements. Then the failures are merely used as a blunt instrument to bludgeon members of the audit department into doing better.

Internal audit functions rarely analyze their shortfalls against success measures to determine the root cause. Too often their response is a simple, "We didn't meet the measures of success this year so, honest, we'll work harder next time." This is a response we wouldn't accept from a client, and one we cannot accept from ourselves.

Make sure you are measuring the right things. Make sure you are meticulously ensuring the credibility of the resulting data. And then make sure you are using the results to effect positive change.

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

FROM EMERGING TO LEADER

Past Internal Auditor Emerging Leaders share how their careers have progressed since they were recognized.

LESLIE BORDELON
Associate Director
Protiviti

ALEX RUSATE
Senior Associate
Risk Consulting, IT
Audit and Assurance
KPMG

How has your career advanced since becoming an Emerging Leader?

BORDELON Since being recognized as an Emerging Leader in 2014, I have received multiple promotions. I'm now an associate director at my firm. I'm still at the same great firm 14 years after starting as an intern in 2005. I also have expanded my family and have a four-year-old son and a two-year-old daughter. Trying to set a good example for them and show them that I have a job that I love and can excel at while also being present and visible for them is a daily goal.

RUSATE Since 2017, I have further developed myself professionally by obtaining my Certified Internal Auditor, Certification in Risk Management Assurance, and Certified Information Systems Auditor designations. Working for my current employer has given me the opportunity to advance my skills, while working alongside industry experts, in an environment that openly promotes and rewards individuals for professional development.

What is your advice for new internal auditors?

RUSATE Never stop learning. You can always obtain more knowledge through certifications, internal business processes, industry level knowledge, etc. I have pursued a variety of internal audit skill sets because I expect that the internal auditor of the future will need to have a strong background in financial, operational, IT, and regulatory matters to keep relevant in the evolving business landscape. New technology, such as intelligent automation, will help scale down the tedious tasks that consume auditors' time and allow them to work on more sophisticated matters that require a higher skill set.

BORDELON Don't overlook the soft skills of listening, being friendly and respectful, asking questions, having a strong work ethic, etc. You can learn the hard skills through research and on-the-job training, but you often cannot teach soft skills. These are usually the distinguishing characteristics between leaders and the status quo.

What skills have helped you most in your career?

BORDELON Maintaining a positive outlook/disposition regardless of the project, client temperament, location—travel or not—or circumstance has been an essential skill that has helped me in my career. I try to look at all situations in a positive light and see all projects as an opportunity to add one more arrow to my quiver of skills. Having this outlook has helped me when deadlines are tough or I'm traveling away from my family. Another skill that has helped me is flexibility. I'm a planner by nature and

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

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

love to know what I'm working on for the next week, year, or even five years. Being a consultant in internal audit has challenged me in that area as my schedule/work commitments change almost daily. Trying to go with the flow and be flexible has been a skill that I've had to develop over time, but one that has served me well in my career.

RUSATE Thinking critically and taking on new challenges with enthusiasm are two traits that have helped me most in my career. Thinking critically has helped me when I have identified opportunities for improvement for unaddressed risks during walkthroughs and testing, and not simply taking management's explanation at face value. Typically, management will know significantly more about a process than you; however, when you combine critical thinking with your holistic knowledge of the company, you can identify risks and opportunities for improvement. Taking on new chal- lenges, such as auditing areas not traditionally reviewed or subject matter that I do not have experience with, has helped to enhance my career. When encountering these situations, I make sure that I have or develop the skills needed to conduct the engagement before accepting it in accordance with IIA Standard 1210: Proficiency. When you have the ability to identify risks, discover process improvements, and step up to address engagements that are important to the chief audit executive, management, or the board, it helps make you a trusted advisor.

What has been your most satisfying moment as an internal auditor?

RUSATE My most satisfying moment was when the global controller reached out to the internal audit team to ask that we help at an advisory level to investigate a potential accounting issue at a manufacturing plant. The figures were not consistent with management's expectation or the fiscal performance of the other manufacturing plants, and management did not have resources available to look into the irregularity. I was assigned to the engagement and was able to determine the root cause of the issue—the implementation of a new ERP system the previous year. Identifying the root cause enabled management to implement corrective actions that led to the company having increased profitability from that plant on a consistent basis.

BORDELON I worked on a project last year with a very tight deadline, a mountain of work, and a good bit of travel. I had a team of all stars, and we worked together to accomplish more than anyone thought possible in such a short period. In fact, we not only completed the project on time, but delivered extra value in many ways and built some great friendships and bonds along the way. It's a project that I won't soon forget.

What frustrates you most in your work?

BORDELON I get frustrated with the negative connotation some people have regarding Sarbanes-Oxley work. I think that work is a fantastic way to learn all aspects of a company, build relationships with clients, and expand your knowledge of an industry. Sarbanes-Oxley work has been invaluable in my career and has afforded me the ability to work on both my hard and soft skills.

RUSATE A challenge in the profession is working with engagement contacts to make sure you maintain a good balance between achieving audit deliverable dates while still being cognizant of their day-to-day responsibilities. Maintaining a mutually respectful relationship with the engagement contacts will help ensure the audit is received in a positive manner and ensure the sustainability of effective audits going forward.

Why do you stay in the profession?

RUSATE I stay in the profession because of the diversity of the subject matter, growth opportunities, and the ability to add value across the entire organization. This profession allows me to gain exposure to functions across businesses, which then enables me to more accurately identify key risks within processes. Furthermore, internal auditing is growing faster than most other professions, according to the U.S. Bureau of Labor Statistics. As reported in the last issuance of the bureau's Occupational Outlook Handbook, employment for internal audit professionals will grow 10% from 2016 to 2026, faster than the 7% national projected average for all occupations. The main reason I stay in the profession is to add value to the organization. Whether it be through identifying risk and working with management to mitigate it down to an acceptable level or identifying process improvement opportunities that drive revenue or cut costs, those are some of the most rewarding aspects of the profession.

BORDELON I stay in the profession because I enjoy the mentoring that my job enables me to participate in and being able to help my clients solve problems and achieve their goals. My colleagues, teams, and mentors are an extension of my family, and I truly feel valued and appreciated in my company and by my clients.

I'm also excited about the future of internal auditing. As companies start to embrace new technologies such as machine learning and robotic process automation, internal audit teams have to really rethink how they approach their work. Adopting more agile practices and understanding both the opportunities and the risks presented by these technologies will put next-generation auditing in a great position to help companies transform their businesses. I'm really looking forward to being a part of that process. Ia

IIA Calendar

IIA CONFERENCES
www.theiia.org/conferences

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

2020

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

JULY 20–22
IIA International Conference
Miami Beach Convention Center
Miami

IIA TRAINING
www.theiia.org/training

NOV. 4–7
Multiple Courses
San Antonio, TX

NOV. 4–13
Audit Report Writing
Online

NOV. 5–8
Tools & Techniques II: Lead Auditor
Online

NOV. 5–14
Critical Thinking in the Audit Process
Online

NOV. 6–15
Fundamentals of Risk-based Auditing (NEW)
Online

NOV. 11–20
Performing an Effective Quality Assessment
Online

NOV. 12–15
Multiple Courses
Las Vegas

NOV. 12–20
CIA Exam Preparation — Parts 1, 2, & 3
Lake Mary, FL

NOV. 12–21
Cybersecurity Auditing in an Unsecure World
Online

NOV. 18–21
Vision University
Chicago

DEC. 2–4
IT General Controls
Online

DEC. 2–13
CIA Exam Preparation —Part 2: Practice of Internal Auditing
Online

DEC. 3–6
Multiple Courses
New York

DEC. 3–6
Multiple Courses
Princeton, NJ

DEC. 3–12
Fundamentals of IT Auditing
Online

DEC. 3–12
Operational Auditing: Influence and Positive Change
Online

DEC. 9–12
Multiple Courses
Orlando

DEC. 9–18
Building a Sustainable Quality Program
Online

DEC. 10–12
COSO Internal Control Certificate
Dallas

DEC. 11–12
Data Analysis for Internal Auditors
Online

DEC. 16–19
Statistical Sampling for Internal Auditors
Online

DEC. 17
Fundamentals of Internal Auditing
Online

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

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

BY CHRIS DOGAS

WELL-DESERVED CRITICISM?

Internal auditors have taken heat from numerous reports, though many don't show the full picture of the profession.

During the last few years, internal auditing has faced significant criticism from both stakeholders and practitioners. Much of it centers around audit effectiveness and the profession's ability to identify and report risks and failures, as highlighted in research from professional service firms. The IIA's own 2019 North American Pulse of Internal Audit points to audit communication deficiencies and potential misalignment with corporate boards on risk areas. But does the profession deserve all of this criticism? Is it truly underperforming?

In my experience, senior management at publicly listed companies mostly views internal audit as a nec- essary evil—a nonessential service function that is either required by a listing exchange or by corporate boards. Otherwise, there is no general appetite to maintain an internal audit function unless the senior executive team, or the board, recognizes the value internal audit adds in providing assurance and improvement opportunities. Because internal audit is not valued, it is not granted sufficient operating budget, which limits the function's ability to cover organizational risks.

Not surprisingly, many surveys of the profession reveal that internal audit struggles to attract and retain talent, is mostly underfunded, and lacks resources, including technology. Gartner's 2018 Audit State of the Function report projected budgets increasing only slightly in 2019 and flat head count for 2019, consistent with prior years. And among respondents to Deloitte's 2018 Global Chief Audit Executive survey, more than 40% said their audit functions lacked skills and talent; plus, only 21% used advanced analytics. How can the profession proactively identify and manage cutting-edge risks in areas such as blockchain, cybersecurity, and fraud when it does not have appropriate capital and technology?

But limited budgets and resources are not the profession's only impediments—lack of control over internal audit's activities and purview, as manifested through our organizational reporting relationships, also presents a problem. At most U.S. publicly listed firms, the chief audit executive reports administratively to the chief financial officer (CFO) and functionally to the audit committee. This configuration risks the CFO providing insufficient budget and other resources and using internal audit to complete projects and tasks not included in the audit plan—activities that might ordinarily fall on other CFO functions—thereby detracting from internal audit's ability to conduct risk-based audits or complete its plan.

Given its limited budgets, inadequate technology resources, understaffing, and lack of autonomy, the profession does not deserve much of the harsh criticism it has received. Only when the audit function is truly independent and empowered will it be able to provide effective support to management and the board, sit at the forefront of risk management, and be able to proactively identify and help remedy corporate misconduct and fraud. Ia

CHRIS DOGAS, CRMA, CPA, CFE, *is vice president of Internal Audit at a large technology company in the New York metropolitan area.*

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

The IIA Congratulates the 2018 Certified Internal Auditor® (CIA®)* Award Winners!

William S. Smith Award – Gold
(Highest Scoring Candidate)
Alexandra Elena Staeben, CIA *USA*

A.J. Hans Spoel Award – Silver
(Second Highest Scoring Candidate)
Ching Nam Leung, CIA *Hong Kong, China*

Kurt Riedener Award – Bronze
(Third Highest Scoring Candidate)
Gannon Burleigh, CIA *USA*

Dr. Glenn E. Sumners Award – Student
(Highest Scoring Student Candidate)
Emilie McRoberts, CIA *USA*

The IIA also recognizes the Certificate of Excellence (Next 10 Highest Scoring Individuals) and Certificate of Honor (Next 50 Highest Scoring Individuals) recipients including, but not limited to:

Certificate of Excellence:*

Airish Ebreo, CIA *Philippines*
John Gentry, CIA *USA*
Jennifer Hurley, CIA *Ireland*
Ng Peng Keong, CIA *Malaysia*
Jennifer Lusa, CIA *USA*
Matthew Owens, CIA *USA*
Brian Reny, CIA *Canada*
Dean Rogers, CIA *USA*
Scott Stepanek, CIA *USA*
Onur Tuzenli, CIA *Turkey*

Certificate of Honor:*

Karla Angeline Andrade, CIA *Philippines*
Jeselle Baldomero, CIA *Philippines*
Natasha Bhatia, CIA *Canada*
Tessalonica Cabeliza, CIA *Philippines*
Reeva Calapatia, CIA *Philippines*
Savio Frederico Ceita, CIA *Brazil*
Christine Croskey, CIA *USA*
Jean-Luc Cueni, CIA *Switzerland*
Michaël Delaet, CIA *Belgium*
Matej Drascek, CIA *Slovenia*
Matthias Dunkel, CIA *Germany*
Sonja Erickson, CIA *USA*
Andreas Friedrich, CIA *Germany*
Miguel Ángel Arévalo Galán, CIA *Spain*
Mark Galley, CIA *Canada*
Justin Gibert, CIA *USA*
Li Hwi Goh, CIA *Hong Kong, China*
Darlene Harris, CIA *USA*
Erin Hayes, CIA *Canada*
Rochelle Hersley, CIA *USA*
Benedikt Hintze, CIA *Germany*
Michael Hostinsky, CIA *USA*
Anna Lawrence, CIA *USA*
Janet Lee, CIA *Canada*
Joonchul Lee, CIA *Korea*
Yan Yin Ian Lee, CIA *Hong Kong, China*
Benjamin Lessard, CIA *Canada*
Sandra Loh, CIA *Singapore*
Leroy Loomis, CIA *USA*
Jason McGowan, CIA *USA*
Kathryn Downs McGuire, CIA *Canada*
Craig McMeechan, CIA *USA*
Vincenzo Mongio, CIA *USA*
Percy Mupita, CIA *United Kingdom*
Marta Nieszporowska, CIA *Poland*
Jorge Orozco, CIA *USA*
Hinrik Pálsson, CIA *Iceland*
Adam Polywka, CIA *USA*
Jennifer Salisbury, CIA *USA*
Sherazade Shafiq, CIA *Austria*
Tomas Slaninka, CIA *Slovakia*
Liam Smith, CIA *Canada*
Nancy Tieu, CIA *Canada*
Daniel Washburn, CIA *USA*
Yan Wu, CIA *Canada*
Han Zhang, CIA *USA*

Join us in congratulating the following individuals for highest achievement on specialty certification exams:

Certification in Control Self-Assessment® (CCSA®)
Joseph Andrew Cox, CIA, CCSA, CGAP, CRMA *USA*

Certified Financial Services Auditor® (CFSA®)
Miguel Ángel Arévalo Galán, CIA, CCSA, CFSA, CRMA *Spain*

Certified Government Audit Professional® (CGAP®)
Wendy Magno, CIA, CGAP *USA*

The IIA congratulates all award winners. It is their dedication to their profession and understanding of the benefits and importance of certification that has led each to achieve these honors.

*Awards are based on individual performance on the core CIA exam parts 1, 2, and 3. With year-round testing, award recipients must pass each segment of the exam on their first attempt within one year of beginning the testing process.

The Institute of Internal Auditors Global

2019-3292

GAM

WHERE LEADERS EVOLVE.

March 16–18, 2020

ARIA RESORT & CASINO | LAS VEGAS, NV

SAVE the DATE!

www.theiia.org/GAM