

Ia

INTERNAL AUDITOR

AUGUST 2018

A PUBLICATION OF THE IIA

Phishing for Information

Blockchain:
What's at Risk?

The One You
Least Suspected

IIA Global Chair:
Elevating the Standards

RANSOMWARE

In a world where attacks are a matter of when – not if – organizations need to have a communication and recovery plan in place.



Accelerate Your Success

Prove Credibility & Proficiency

CERTIFIED FACT: As the only globally recognized certification for internal auditors, becoming a Certified Internal Auditor® (CIA®) proves skill, value, and understanding of the *International Standards for the Professional Practice of Internal Auditing* and how to apply them. When CIA follows your name, you earn more respect, promotions, and money!*

Improve your credibility and proficiency. [Learn more.](http://www.theiia.org/CIA)

www.theiia.org/CIA



*According to The IIA's 2017 Internal Audit Compensation Study (based on U.S. responses).

Agile audit management with Thomson Reuters

Capitalize on change and help business partners achieve strategic business objectives.

At Thomson Reuters we recognize that no two audit functions work the same way. With Thomson Reuters Audit Management, on our Connected Risk platform, we provide a flexible audit solution that easily adapts to your business requirements.

Using Audit Management empowers your teams with assessments that align with how your business thinks about risk. The solution's workflow can adjust with the evolving needs of your audit team, and provides a simpler way for you to adapt to changing audit practices.

Audit Management, now with more flexibility, more options, and more connectivity to other parts of your business.

risk.tr.com/audit-management



The intelligence, technology and human expertise
you need to find trusted answers.



the answer company™
THOMSON REUTERS®



Get all the tools and resources to audit more effectively.

Global industry experts at The IIA develop, document, and deliver the standards of the profession, along with all the tools to understand and apply them. Aligning with the *International Standards for the Professional Practice of Internal Auditing* can help internal auditors of all levels and sectors perform their jobs more effectively.

[Practical Tools](#) | [Latest Resources](#) | [Training Courses](#)

Standards Practice Makes Sense
www.theiia.org/HaveStandards

 **The Institute of
Internal Auditors**



FEATURES

28 COVER Held Hostage Victim organizations are paying a high price for ransomware attacks.
BY ARTHUR PIPER

34 Pulling Strings High-level hackers are using social engineering tactics to manipulate employees into giving up vital information.
BY RUSSELL A. JACKSON

41 Internal Audit and the Blockchain There's more to the blockchain than bitcoin, and auditors have much to learn about how it works. **BY LORRAINE LEE, KIRK FIEDLER, AND RICHARD MAUTZ**

46 The Ones You Least Suspect Internal auditors must be alert to the red flags of fraud,

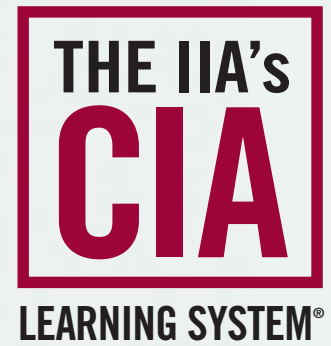
even when they point to the organization's most trusted employees. **BY RICHARD F. CHAMBERS AND DEANNA F. SULLIVAN**

52 A Standard of Performance **NAOHIRO MOURI**, the 2018-2019 chairman of The IIA's Global Board of Directors, urges internal auditors everywhere to "Emphasize the Basics – Elevate the *Standards*."

58 Women at the Top Six internal audit leaders share how they climbed the professional ladder. **BY JANE SEAGO**



DOWNLOAD the Ia app on the App Store and on Google Play!



A System for Success.

Prepare with Confidence & Convenience.

The IIA's CIA Learning System is an interactive review program, combining reading materials and online study tools to teach and reinforce all three parts of the CIA exam. It's updated to align with the latest industry standards, including the International Professional Practices Framework (IPPF) and The IIA's *International Standards for the Professional Practice of Internal Auditing*.



Prepare to Pass. www.LearnCIA.com



2018-0267

DEPARTMENTS



7 Editor's Note

8 Reader Forum

71 Calendar

PRACTICES

10 Update CIOs prioritize locking down data; U.S. agencies uncertain about cybersecurity qualifications; and retailers report less inventory loss.

15 Back to Basics Audit reports should both inform and influence.

19 ITAudit Technology is a valuable audit tool.

22 Risk Watch The heavy lifting of GDPR compliance is just beginning.

25 Fraud Findings Crime doesn't pay, again.

INSIGHTS

64 Governance Perspectives ERM often requires a compelling sales pitch.

67 The Mind of Jacka Internal auditors need to think about how they think.

68 Eye on Business Are auditors taking full advantage of today's analytics?

72 In My Opinion Internal auditors should plan for political pressure.

ONLINE InternalAuditor.org



Women in Leadership

Watch several female audit executives from our cover story discuss their rise to the top, as well as those who influenced and inspired them along the way.

Crisis Overconfidence

According to a new survey, a majority of organizations face more crises today than they did 10 years ago – but many may overestimate their ability to respond.

The Audit Bots As organizations rely more on robotic process automation, internal auditors need to be involved in assessing its risks and learn how to use it, themselves.

Unsafe Inspectors Auditors accuse city vendors of multiple frauds and signing off on fire code inspections they may not have performed.

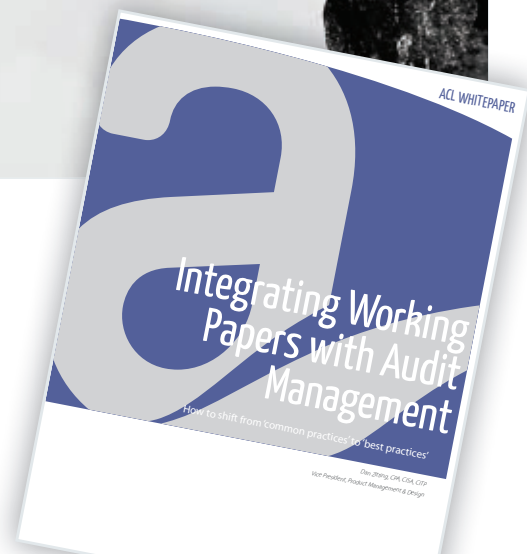




CLOSE THE AUDIT PERFORMANCE GAP

How to shift working papers from
'common practices' to 'best practices'

Download at acl.com/workingpapers »





THE HUMAN FACTOR

I'm a big fan of the TV series *Westworld*. For those who haven't seen it, HBO's science fiction thriller takes place in a Western-themed, no-holds-barred amusement park where guests interact with lifelike robotic hosts. The show's many plot twists keep viewers guessing, though eventually we learn there's much more going on than just gun fights and pleasure seeking. The park's creators have been quietly taking advantage of guests to carry out a hidden agenda. And while the plan relies in part on *Westworld*'s futuristic technology, one of its main tools is simple human deception.

Beyond the realm of fiction, of course, people's susceptibility to deception and manipulation is a real-world concern for organizations — particularly when it comes to cybersecurity. With a phone call, email, social media exchange, or in-person conversation, skilled social engineers can gain the trust of their victims to commit fraud or other organizational crimes. And as Kimberly Hagara, vice president, Audit Services, at University of Texas Medical Branch, notes in "Pulling Strings" (page 34), the attackers are becoming increasingly sophisticated. "Now the tactics are much more trust-based," she says. "Getting into an organization or a system relies more on human interaction."

In some cases, the attackers leverage systems access to hold the organization's data hostage. Their success depends not only on malicious software, known as ransomware, but often on the perpetrators' ability to deceive. According to a recent survey by security firm SentinelOne, nearly 70 percent of successful ransomware attacks in 2017 resulted from hackers gaining access to enterprise networks by phishing via email or social media.

In our cover story, "Held Hostage" (page 28), author Arthur Piper examines the risk of ransomware, how to respond to an attack, and considerations for prevention and detection. The article also stresses that employees often represent the greatest vulnerability to these types of attacks. With that in mind, risk management advice includes ensuring training is provided to all personnel and that policies on responding to ransomware incidents have been well-communicated.

Cyberattacks don't have to be high-tech to present a real threat. Despite all the sophisticated tools available for carrying out an attack, crafty perpetrators can weasel their way through even the best defenses with simple techniques that exploit human psychology. Ironically, in the age of artificial intelligence and advanced digital security, preventing cybercrime often comes down to a deeper understanding of nontechnological, human factors. The weakest link in the security chain is often the employee who opens the door, physical or virtual, to an intruder. And when that happens, to borrow from *Westworld*'s season two tag line, "chaos takes control."

A handwritten signature in black ink that reads "David Salierno". The signature is fluid and cursive.

David Salierno

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



that Weinstein was helpful and agree that the behavior he's accused of is reprehensible. In no way did I intend to portray him in a positive light or suggest that he should be given credit. Instead, I was pointing to the Weinstein situation as a catalyst for the #MeToo movement, given how many brave women have come forward since the situation came to light.

“Is the definition of sexual harassment changing?” I believe that it is. The #MeToo movement on the back of the Weinstein scenario is highlighting a new definition of *sexual harassment*, the unwanted advances, and sleazy remarks and innuendo—none of which are appropriate in any workplace.

Employers need to review any policies currently in place, and if they do not have an appropriate policy then they need to establish one. And as importantly, they need to promulgate it effectively so there can be no misperception of what is and isn't acceptable in the workplace—or face the potential of litigation.

HARMONY BALL comments on Russell Jackson's "Into the Light" (June 2018).

Auditing Culture

Doug Anderson's article on auditing culture is a valuable contribution. I offer one qualifier to be sure it's not misunderstood. What he calls “strong evidence” (auditors' perceptions of the culture through their in-depth exposure to it) is essential, but it is less persuasive to many stakeholders than his “weak evidence” (survey results, turnover statistics, etc.) The truth is that neither stands by itself. We need to gather and correlate all the evidence from a variety of sources and techniques. We can then progressively enrich the understanding of our organization's culture for ourselves and our stakeholders.

JIM ROTH comments on Douglas Anderson's "Beneath the Surface" (June 2018).

The thoughts in this article are good as far as they go, but like so many articles on culture, it focuses on ethics. Very few businesses are in the ethics business, so it's unlikely that a focus on ethics will represent the business culture. To audit culture, auditors need to assess where the business focus is placed. Ethics is part

#MeToo

Harvey Weinstein in no way helped women in the workplace. The brave individuals who spoke up about his abhorrent actions are responsible for helping women in the workplace. It is distasteful to imply, let alone state, that he or anyone else who commits actions like those of which he has been accused can be responsible for helping women in the workplace.

ALISON B. comments on Russell Jackson's "Into the Light" (June 2018).

AUTHOR: Thank you for your comments. I understand your reactions to the notion



AUGUST 2018
VOLUME LXXV:IV

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

CONTRIBUTING EDITORS

Wade Cassels, CIA, CCSA, CRMA, CFE
Kayla Flanders, CIA, CRMA
J. Michael Jacka, CIA, CPUC, CFE, CPA
Steve Mar, CISA, CISA
Bryant Richards, CIA, CRMA
James Roth, PHD, CIA, CCSA, CRMA
Charlie Wright, CIA, CPA, CISA

EDITORIAL ADVISORY BOARD

Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, FCPA, FCGA, FCMA
Mark Brinkley, CIA, CISA, CRMA
Robin Altia Brown
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Wade Cassels, CIA, CCSA, CRMA, CFE
Faizal Chaudhury, CPA, CGMA
Daniel J. Clemens, CIA
Michael Cox, FIA(INZI), AT
Dominic Daher, JD, LL.M.
Haylee Deniston, CPA
Kayla Flanders, CIA, CRMA
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA

Jorge Gonzalez, CIA, CISA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
Karin L. Hill, CIA, CGAP, CRMA
J. Michael Jacka, CIA, CPUC, 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
Dennis McGuffie, CIA
Stephen Minder, CIA
Jack Murray, Jr., CBA, CRP
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Manish Pathak, CA
Bryant Richards, CIA, CRMA
Jeffrey Ridley, CIA, FCIS, FIA
Marshall Romney, PHD, CPA, CFE
James Roth, PHD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debora Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PHD, CPA
Glenn Summers, PHD, CIA, CPA, CRMA

Sonia Thomas, CRMA
Stephen Tiley, CIA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoof, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CISA, CRMA
Rodney Wright, CIA, CPA, CISA
Benito Ybarra, CIA

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

IIA CHAIRMAN OF THE BOARD
Naohiro Mouru, CIA, CPA



PUBLISHED BY THE
INSTITUTE OF INTERNAL
AUDITORS INC.

CONTACT INFORMATION

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

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

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

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

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

Authorization to photocopy is granted to users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the current fee is paid directly to CCC, 222 Rosewood Dr., Danvers, MA 01923 USA; phone: +1-508-750-8400. *Internal Auditor* cannot accept responsibility for claims made by its advertisers, although staff would like to hear from readers who have concerns regarding advertisements that appear.

of it, of course, but what about quality, safety, service, commitments, etc.? These factors should be included when looking at culture, plus whatever other specific values are promulgated by the company.

RICHARD FOWLER comments on Douglas Anderson's "Beneath the Surface" (June 2018).

Improving Client Relationships

I've often had similar ideas in my head, and appreciate that Grace Wu articulated something that can have an immediate impact on internal audit's credibility and standing. She hit the key points needed to improve our relations with internal clients: how we communicate with the business, coordination across lines of defense, and communicating an enterprisewide view of risk. This was followed up by emphasizing an approach that addresses "why clients

should care" and the need to include more risk-based information to put the "issues" in a context that the business and high-level stakeholders understand.

MICHAEL WALKER comments on Jingwen (Grace) Wu's "Risks Speak Louder Than Issues" ("In My Opinion," June 2018).

Auditing Remotely

One very effective means of auditing remotely is to use data analytics to examine all the transactional activity within a business process area. Complete populations of financial and operational activities can be tested for compliance with the controls that are meant to be in place. Visual and statistical analytics can be used to identify anomalies and risk indicators. All of this can be performed remotely and then—based on the results—decisions made as to when,

where, and even if it is necessary to perform an on-site audit.

JOHN VERVER comments on Matthew Suhovsky's "Audits From Afar" (InternalAuditor.org).

Manage Expectations

With a statistical sample, it is more obvious that we cannot find every exception or provide complete assurance. However, even reviewing 100 percent of a population does not guarantee compliance with all aspects of a process. It might just denote that the testing attributes are as expected. Our job is to help our stakeholders strengthen their controls, not make guarantees, and we need to make sure this is discussed during our audits.

FRANK HOLLOMAN comments on the Chambers on the Profession blog post, "Internal Auditors Can Audit Anything—but Not Everything" (InternalAuditor.org).



Engage and Connect Globally

Gain a competitive edge with unique IIA advertising and sponsorship opportunities as diverse as the 190,000 members in the 185 countries we serve.

Contact +1-407-937-1388 or sales@theiia.org for more information.

www.theiia.org/advertise

 **The Institute of
Internal Auditors**

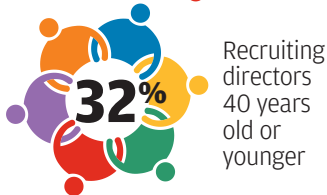
2015-1635

U.S. executives worry about trade... Government can't identify cyber talent... The consequences of employee speech... Retail inventory loss is shrinking.

Update

BANKS SEEK BOARD DIVERSITY

Directors say adding women, minorities, and younger members would broaden board composition.



Source: *Bank Director*, 2018 Compensation Survey



CIOs PRIORITIZE SECURITY AND DATA

Tech leaders are focused on locking down company data.

Seeking to increase compliance with new data privacy protection and security regulations and to avoid costly data breaches, organizations are devoting increased attention to data and cybersecurity, according to a recent survey. The 2018 Harvey Nash/KPMG CIO Survey, based on responses from nearly 4,000 chief information officers and other technology leaders, found that almost 25 percent more respondents than in 2017 are prioritizing cybersecurity improvements in light of growing threats.

Increased organizational focus on cyber threats stems in part from heightened board

awareness about potential attacks. “Protecting the business from a cyberattack has jumped farther up the boardroom agenda than any other item, and IT leaders are being encouraged to make their defenses the best that they can be,” says Akhilesh Tuteja, global cybersecurity services co-leader, KPMG International.

Data trust and privacy threats are also among IT leaders’ greatest concerns. And while many firms are prioritizing data security in light of legislation such as the European Union’s General Data Protection Regulation (GDPR), 38 percent of those surveyed in April said they would not achieve

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

IMAGES: TOP: SERGEY NIVENS / SHUTTERSTOCK.COM; LEFT: AMERICA365 / SHUTTERSTOCK.COM

GDPR compliance by the May 25 deadline. Additionally, 77 percent say they are “most concerned” about organized cybercrime—an increase from 71 percent last year.

Concerns about network safety have led to a large demand for “security and resilience” skills. These two areas represented the largest increase in skill shortages, climbing 25 percent since last year. Moreover, as organizations increasingly move toward digital

platforms and solutions, more than one-third of respondents’ organizations say they cannot hire and develop people with the digital skills they need.

The survey also examined leadership profiles, noting a slight uptick in the number of women in charge of IT. According to the results, women hold 12 percent of IT leadership roles and 21 percent of technology positions overall. — **D. SALIERNO**

TRADE TURMOIL

Business impact of tariffs concerns U.S. executives.

More than one-third of U.S. business executives are worried about a potential trade conflict between the U.S. and its trade partners, notes the American Institute of CPAs’ (AICPA’s) second quarter 2018 Economic Outlook Survey. The survey polled 831 CEOs, chief financial officers, controllers, and other decision-makers in May, before the U.S. announced tariffs on steel and aluminum for some trading partners.

“Most business executives—52 percent—said a more protectionist approach to trade policy would have a negative impact on the U.S. economy,” says Arleen Thomas, the AICPA’s managing director of Americas Market, Global Offerings, and Chartered Global Management Accountant Exam.

Specifically, 40 percent say U.S. trade tariffs and potential retaliation by trade partners would impact their businesses. Among those executives, nearly one-fourth say the impact would be significant.

Executives’ greatest trade concerns are a global economic slowdown, rising business costs, and rising prices on goods and services their companies sell. — **T. MCCOLLUM**



86%
**OF CRISIS
MANAGEMENT AND
RISK EXECUTIVES**
say their organization’s crisis management preparedness is mature, yet only

17%
**HAVE TESTED THEIR
ORGANIZATION’S
ABILITY**
to deal with a corporate scandal, and

22%
**HAVE TESTED
WHETHER IT COULD
MANAGE A
PRODUCT RECALL.**
“It is crucial for organizations to be ready to respond with agility to multiple scenarios that have been rehearsed and tested,” says Sam Balaji, global leader, Financial & Risk Advisory, at Deloitte.

Source: Deloitte, Stronger, Fitter, Better: Crisis Management for the Resilient Enterprise

FEDERAL CYBER WORKFORCE UNCERTAIN

Agencies struggling to identify existing talent and future needs are raising their cyber risk.

U.S. federal government agencies may not be prepared to head off malicious attacks because they have an inadequate understanding of their cyber workforce and needs, according to a U.S. Government Accountability

Office (GAO) report. “A key component of the government’s ability to mitigate and respond to cyber threats

is having a qualified, well-trained cybersecurity workforce,” the report says.

The GAO notes that many agencies have missed deadlines and reported gaps in developing a coding structure to track cybersecurity positions and procedures for assigning codes to federal civilian cybersecurity positions—provisions of the Federal





Cybersecurity Workforce Assessment Act of 2015.

As of March, 21 of the 24 agencies covered by the Chief Financial Officers Act submitted required baseline assessment reports to the U.S. Congress. According to the GAO's analysis of those reports, four agencies failed to report information such as "the extent to which personnel without certifications were ready to obtain them or strategies for mitigating any gaps." The Department of Homeland Security, the U.S. Department of Housing and Urban Development, and the Small Business Administration did not submit assessments because of a lack of tools and resources.

The GAO issued 30 recommendations to 13 agencies that fell short on how to improve compliance. Many of the recommendations focused on evaluating the level of preparedness for cybersecurity personnel not currently holding certifications to take certifications exams and identifying strategies for mitigating identified gaps. Agencies also need to identify IT and cybersecurity-related noncivilian positions, and assign employment codes to those positions.

Without an adequate understanding of its cyber workforce and training needs, agencies are challenged to ensure they have the necessary personnel to protect critical infrastructure and federal networks from cyber threats, the report states. —S. STEFFEE

NOT WITHOUT CONSEQUENCES

U.S. employers can fire at will for speech made on or off the clock, says Veronica Nannis, principal and litigation practice group manager at Joseph, Greenwald & Laake P.A.



In light of Roseanne Barr's firing following her controversial tweets, how can organizations limit what employees post on social media?

The First Amendment of the U.S. Constitution does not apply here because it limits the government's censorship of speech. There is no "freedom of speech" blanket protection while an employee is on the clock for a private employer. Employers can limit speech made at work and on the clock. An employer can proscribe certain speech in the workplace, just as it can mandate a specific dress code. But what many don't realize is that while

an employer cannot limit or prevent speech outside the workplace, that speech can still have employment consequences. An employer can fire for speech made outside the workplace and off the clock in most at-will states. "At will" means that, absent a contract, certain union protections, legal prohibition, or public policy, an employer can fire for any reason, or no reason at all. In an at-will state, a private employer does not need a reason to fire. So, while an employee can post to social media at will, a private employer can generally fire at will, as well. A few states have some laws that do protect limited out-of-work speech, but these are a small minority. So, speech may be free but it is not without consequences.

RETAIL SHRINK HAS SHRUNK

Merchants report reduced inventory loss.

Losses from theft, fraud, and other abuses—collectively known as retail "shrink"—dropped from \$48.9 billion in 2016 to \$46.8 billion in 2017, according to the annual National Retail Security Survey published by the National Retail Federation and the University of Florida. Shoplifting and organized

retail crime (ORC) topped the list of causes behind retail shrink.

Overall, shrink averaged 1.33 percent of sales, compared to 1.44 percent in 2016. Fifty-nine percent of retailers surveyed say shrink is either flat or decreasing, up from just over half in last year's report. Still, 41 percent say shrink is growing, though that proportion is down nearly 10 percent from 2016.

Shoplifting and ORC accounted for 36 percent of shrink, followed by internal employee theft (33 percent), administrative paperwork errors (19 percent), and vendor fraud or mistakes (6 percent). The biggest losses stemmed from robberies, averaging more than \$4,200 per incident. Employee theft and shoplifting/ORC averaged \$1,203 and \$599 per incident, respectively. The proportion of respondents experiencing an average loss of \$300 or more dropped from nearly half in 2016 to one-third in 2017. —D. SALIERNO



17th Annual Society of Corporate Compliance and Ethics

COMPLIANCE & ETHICS INSTITUTE

OCTOBER 21-24, 2018 | LAS VEGAS



Experience the Difference

1800+
ATTENDEES

150+
SPEAKERS

10 LEARNING
TRACKS

100+
SESSIONS

Attendees have the opportunity to learn about current hot topics including:

- > Global Compliance
- > Internal Investigations
- > Risk Assessment
- > Cyber Security
- > Whistleblowers
- > Retaliation
- > SOX Compliance
- > Privacy Programs
- > Regulatory Compliance
- > Fostering a Compliance Culture

complianceethicsinstitute.org



SCCE[™]
Society of Corporate
Compliance and Ethics

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

Learn From The Leader.

.....
IIA TRAINING – ALL PLATFORMS OPEN

As an internal auditor, you'll always find there's more to discover. And while on the job training is par for the course, sometimes learning the latest lessons from the industry leader is the best course of action. The IIA delivers innovative, quality, and convenient internal audit training and development for all skill levels. The flexible training platforms focus on individual auditor training needs, as well as existing and emerging issues to ensure that internal auditors receive the knowledge and proficiency required to provide the highest level of auditing assurance, insight, and objectivity possible.

Schedule training on a platform perfect for your station www.theiia.org/Training



ONDEMAND / ON-SITE / IN-PERSON / ONLINE

Back to Basics

BY JONNIE T. KEITH EDITED BY JAMES ROTH + WADE CASSELS

PRODUCING QUALITY AUDIT REPORTS

Audit reports require thought and effort to not only inform audit clients, but to influence them, as well.

The audit report represents the end result of weeks of reviews, analyses, interviews, and discussions. It provides important information to audit clients about the area reviewed by internal audit. More importantly, it provides details to management about significant issues that need to be addressed. How well internal auditors communicate that information is critical to getting their client's acceptance of findings and their agreement with audit recommendations.

Quality reports require thought and effort. Auditors should consider who will read the report, what they will do with it, what level of detail is necessary, what the organization's culture and norms call for, and if industry-specific language is necessary. IIA Standard 2420: Quality of Communication says communications should be accurate, objective, clear, concise, constructive, complete, and timely.

Accuracy

Inaccurate information could adversely impact the credibility of the entire audit report, so accuracy is critical. All of the numbers should be correct, the information should be factual, and documentation verifiable. There may be disagreement on what the numbers or facts mean, but there should never be an argument about their accuracy.

Accuracy is enhanced by appropriate supervision of the audit engagement. The IIA's *International Standards for the Professional Practice of Internal Auditing* requires adequate supervision of engagements, and part of that includes verification of numbers and facts. Accurate and precise information lessens the chance of a misunderstanding.

Objectivity

Objectivity is the second most important quality behind accuracy. If readers feel that the report is not objective, it could undermine the confidence they have in

the report. And while the report may be objective, the subtle use and placement of certain words can appear to show bias. This can be crucial to whether the reader accepts the auditor's conclusions and recommendations.

Objective words are precise. They speak to the facts and can be supported by evidence. Biased words are subject to generalization and distortion of information. For example, the statement, "Very confidential files were just stuck in a drawer where anyone could get to them," is biased and opinionated. A more objective statement would be, "Confidential files were stored in an unsecure drawer to which unauthorized personnel had access."

Reports must be clear enough for readers to understand without having to refer to anything else. Language should include precise modifiers and clear technical terms.

Precise Modifiers A modifier is a word or phrase that

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



Featuring

Internal Auditor Blogs

Voices with viewpoints on the profession

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

Chambers on the Profession:

Seasoned Reflections on Relevant Issues

From the Mind of Jacka:

Creative Thinking for Times of Change

Solutions by Soileau:

Advice for Daily Audit Challenges

Points of View by Pelletier:

Insights and Innovations From an Insider

READ ALL OF OUR BLOGS. Visit InternalAuditor.org.





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

alters the meaning of another word. Generally, the modifying word should be as close as possible to the word it is modifying. Otherwise, the modifying word could attach itself to a word that was not intended to be modified. This can subtly alter the meaning of the sentence or make it ambiguous.

For example, see how the placement of the word *almost* changes the meaning of the sentence: “The plane almost failed every inspection” vs. “The plane failed almost every inspection.” The first sentence leads readers to believe that the plane passed every inspection, whereas the second sentence indicates that the plane rarely passed any inspection.

Clear Technical Terms Auditors should consider spelling out acronyms, replacing technical terms with nontechnical words, and embedding definitions within the sentence. For example, “The audit department uses the COSO framework, a comprehensive list of controls, as a standard for controls and risks.”

Conciseness

Readers always appreciate conciseness, but it should not mean cutting down on information. It means using fewer words to convey the same information. Some things that impact conciseness include drawn-out verbs, overstated language, and redundant modifiers.

Drawn-out verbs turn verbs into noun phrases. They often, but not always, contain a noun with the “tion” ending and require a preposition. In most cases, the phrase can be replaced with one word. For example, “Make a determination of ...” can be replaced with the word “Determine.” And “Perform a verification of ...” can be replaced with “Verify.” Replacing the words conveys the same information with fewer words.

Overstated language uses longer, more complicated words where simpler, shorter words will do. For example, “Due to the fact ...” can be replaced with “Because.” And “In order to ...” can be replaced with “To.” Again, this doesn’t detract from the information.

Redundant modifiers turn a simple adjective into a long phrase. For example, the phrase, “In the month of May ...” can be replaced with the words “In May” And the phrase, “On a daily basis ...” can be replaced with “Daily.”

Constructiveness

Constructiveness primarily refers to the audit recommendations, which should give audit clients information to correct the current problem and also address the root cause so as to mitigate future occurrences. For example, departmental procedures call for inventory to be reconciled monthly. The audit determined that there were three months that did not get reconciled, and the manager explained that the person who

normally does it was on sick leave and had no backup. In the audit report, the recommendations read:

“The inventory manager should review the three months of inventory to ensure its accuracy. Further, the manager should cross-train another person in the department to serve as a substitute when the primary person cannot reconcile the inventory account.”

The recommendation addresses the three months that were not reconciled, the root cause, and cross-training another employee to ensure this does not happen again.

Giving management information to correct the problem and keep it from happening again adds to the quality of the report and shows how audit adds value to the organization.

Completeness

Everything the reader needs to make an informed decision should be included in the report, and no significant information should be left out. The auditor must not omit valid information because it does not support his or her points. Present all the facts and allow the reader to decide.


Standard 2410 states, “Communications must include the engagement’s objective, scope, and results.” So, the report is not complete without the reason for the audit, the final conclusion based on the evidence reviewed, and the amount of evidence reviewed to come up with the conclusion.

Timeliness

Auditors should complete and issue reports as soon as possible to give the audit client a chance to address the issues timely. Timeliness may vary based on things like the audit resources needed to complete the audit, the complexity and significance of the audit, the report review process, and other factors.

If serious issues need to be communicated before the report is completed—such as customer or employee safety or significant loss of assets—the auditor should immediately issue an interim report or memo to allow the client the opportunity to address the problems as soon as possible. The interim report or memo can be referenced in the final report.

Valued Reports

An audit report must be accurate and objective; flexible enough to communicate sometimes complex information to various levels of people; and able to withstand the scrutiny of peer reviews and other assessments, depending on the industry. A quality audit report aids audit clients in making informed decisions, so taking the time and effort to put it together benefits the audit client and auditor. 

JONNIE T. KEITH, CIA, CFE, CGAP, is an audit consultant at *JonSherr Enterprise in Atlanta*.



Audit Management Software

✓ **No Gimmicks**

✓ **No Metaphors**

✓ **No Ridiculous Claims**

✓ **No Clichés**

A satellite view of Earth at night, showing the curvature of the planet and the glowing lights of cities and continents against the dark background of space.

Just Brilliant Software.

Find out more at www.mkinsight.com

Trusted by Companies, Governments and Individuals Worldwide.

PLUGGING MORE VALUE INTO INTERNAL AUDITS

Leveraging technology can enable practitioners to provide a deeper analysis of organizational risks.

A common response to corporate scandals caused by significant control lapses is to question the performance and value of audits performed by internal audit, particularly the department's role in providing assurance on enterprise risk management activities. To better identify and assess these types of risks, internal audit needs to provide more valuable audits that evaluate risks and controls, identify gaps, determine root causes, and recommend improvements.

Taking data privacy as an example, internal audit is expected to evaluate the security of databases where information is stored and determine who has access, how that information is used, and with whom it is shared. Additionally, auditors must provide assurance that the information is not being shared with anyone who should not have access to it. Yet, due to staffing limitations and tight deadlines

for providing deliverables, internal audit departments often don't have time to provide in-depth reviews on emerging risks.

One way to provide this service is to use technology to automate routine reviews so that they can be performed faster. This can free internal auditors to examine areas they may not have previously audited. Reporting on controls for these once-unexamined areas can provide assurance that controls are operating as designed or identify gaps where improvements are needed. Internal audit can therefore report valuable information about risks and controls that has not been included in prior audit reports.

A Large-scale Analysis

Value-added auditing is a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. It requires internal auditors to

analyze risks and controls to identify the root cause of the ineffectiveness, recommend corrective action, and focus on continuous improvement.

To perform more valuable audits, internal auditors need time to focus on the overall risks to the organization, while obtaining detailed information to determine the root cause of the finding, not just identify the resulting error. Only then can auditors recommend functional improvements and follow up to ensure they have been implemented. By taking time to probe and understand the business risks and collaborating to develop functional solutions to challenges faced, auditors can move from being a reviewer to a business partner working to resolve problems and simplify complex tasks.

But internal audit must overcome certain obstacles to perform value-added audits such as having a check-the-box mentality, managing concurrent

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



think machine. **ACT AUDITOR.**

The IIA has the resources to help you learn how disruptive technologies and internal audit intersect to propel your career to the next level. From the latest guidance to courses and conferences — and from books to blogs — we offer technology opportunities to help bring robot-like precision and accuracy to your internal audit activity.

Start with a new Internal Audit Foundation report, *Artificial Intelligence: The Data Below*.
Download the **FREE** report at www.theiia.org/ThinkMachine.



TARGETED RESOURCES | LATEST TRAINING | CUSTOMIZED EVENTS



TO COMMENT on this article,
EMAIL the author at bernadette.calhoun@theiaa.org

projects with limited resources, and breaking down information silos. Auditors must communicate relevant information to clients timely, and the department must be flexible enough to respond to changes and emerging risks. By automating routine reviews, auditors can work within the same constraints yet still issue an opinion on controls that may not have been examined previously. Automated reviews also may help auditors identify gaps or risks where there is no mitigating control. Such gaps could expose the organization to potential threats. The time gained to focus on additional areas can enable auditors to provide a larger scale analysis that encompasses strategic organizational goals.

Putting Data to Work

Technology is key to performing more valuable audits. Automating routine reviews allows for the quick identification of outliers in regularly examined data, a focused review on those specific occurrences, and budgeted time to examine additional areas. In lieu of spending time examining an excessive number of transactions that fall within the expected tolerance, internal auditors can define the normal tolerance and use software to identify the outliers and a small, random sample of normal transactions, then focus the remaining time on examining new areas, such as information security and privacy. Moreover, by leveraging technology, internal audit can set an example for how innovation enhances performance.

Automation can give auditors more time to question what is being done and why.

Electronic Workpapers Easily shared workpapers may allow a subsequent audit to leverage information identified in a previous exam. By using templates to document audit results, auditors do not have to recreate templates for each review. Linking documents, such as workpapers, support documentation for findings, and policies, allows for a quicker review and access to standards used in the testing and evaluation portions of the audit.

Data Mining Internal auditors should automate reviews to allow for continuous monitoring of routine tasks and to easily identify trends and anomalies that may require additional attention. For example, creating dashboards or setting up

alerts can enable internal auditors to quickly identify transactions occurring outside the normal range. When continuously monitored, those outliers can be identified, examined, and, if necessary, corrected sooner than discovering them through a scheduled audit. Detecting outliers faster could minimize the impact of transactions that should not be allowed to continue.

Analytics Analyzing data can enable internal auditors to determine the impact of control weaknesses and the frequency in which they occur. This allows auditors to put issues in perspective and provide clients with a view of risks when there is a failure to comply. By analyzing performance trends and patterns, internal auditors can demonstrate how risks change by time and region. The analysis also can help clients understand the effectiveness of controls as well as determine where corrective actions are needed. Additionally, data analysis can assist management with regulatory and policy compliance in a way that minimizes duplication of efforts.

To analyze data effectively, internal auditors should set parameters to identify the data that lies outside the normal parameters. This can quickly show where the outliers and risks lie, allowing auditors to devote time to examining these risks.

Dashboards Auditors can use dashboards as a visual method of identifying anomalies and comparing them to other data.

Dashboards can demonstrate current versus future states. Moreover, visual demonstrations work well for reporting, explaining findings to decision-makers, and driving change.

Finding More Value

Technology has an additional way to make audits more valuable. By automating routine tasks, internal audit departments can be better structured to perform audits that are more useful for improving governance, risk management, and control processes. This automation can give auditors more time to question what is being done and why, compare current practices to best practices and industry standards, and evaluate whether there is a more innovative approach. Internal auditors should explore opportunities to use existing technology to automate routine reviews, add value to the organization by reporting on additional areas, and minimize the impacts of risks to their organization. [Ia](#)

BERNADETTE CALHOUN, CFE, is a quality audit consultant at Lincoln Financial Group in Atlanta.

GDPR AND INTERNAL AUDIT

Auditors can help their organization navigate the compliance risks posed by Europe's General Data Protection Regulation.

Now that the May 25 deadline has passed to comply with the European Union's (EU's) General Data Protection Regulation (GDPR), compliance executives may be breathing a sigh of relief. Yet the real compliance work is only beginning.

GDPR consolidates the EU's personal data privacy protection laws and redirects the way organizations approach data privacy. It greatly expands the privacy rights of E.U. citizens and residents, and it applies to any organization that does business with those individuals, regardless of its location. Organizations that don't comply with GDPR face penalties of up to €20 million or 4 percent of annual worldwide turnover, whichever is greater.

Compliance will require continued focus and effort. Internal audit can help the organization mitigate GDPR compliance risks by identifying ways to improve controls,

raising risk awareness, and assuring compliance.

Improving Controls

Internal audit can help the organization shift from the preparation phase to the implementation phase of GDPR. The regulation specifically requires organizations to focus on these control-oriented topics:

- ➔ *Accuracy and quality* requires organizations to ensure data is accurate and up-to-date and that individuals can correct their records.
- ➔ *Security and privacy by design* requires organizations to document decisions taken to inform EU residents about how their data will be used and restricted. They also must implement technical, administrative, and physical security/privacy controls to mitigate potential harm.
- ➔ *Security safeguards* ensure that technical and organizational measures are

implemented for privacy and security.

Internal audit should work with management to identify relevant controls over data entry, assess the accuracy of information and recommend improvements, and strengthen controls that prevent and detect data errors.

Raising Risk Awareness

The direct risks associated with GDPR relate to potential fines and reputational impact. However, by digging into the regulation's purpose, internal auditors can see other data protection risks.

Monitoring, Measuring, and Reporting

Organizations must have a data protection officer (DPO) to lead privacy and compliance efforts. Among the DPO's tasks are reporting on compliance monitoring, training staff, and ensuring privacy compliance audits take place. The organization must perform data privacy impact assessments when new technologies

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



TO COMMENT on this article,
EMAIL the author at jan.hertzberg@theia.org

and systems are used, provide timely data breach notifications, and report on the use of third-party processors.

Prevent Harm GDPR imposes sanctions and penalties on organizations that process data unlawfully or fail to deploy safeguards. In addition, individuals may request that the organization remove their personal data from automated processing and profiling.

Breach Management Organizations must put processes in place to notify persons no later than 72 hours after they discover a data breach, if it is determined that the breach will result in a high risk of privacy harm to those individuals.

Openness, Transparency, and Notice Organizations must keep data for specific and legitimate purposes and notify persons about how the organization will use their data. Organizations also must inform individuals of safeguards applied when personal data is transferred to a third country.

Individual Participation EU residents may request access to data, obtain a copy of the data held, and withdraw consent to use personal data as long as withdrawal does not result in legal violations. Individuals may object to the use of their data for direct marketing and profiling, and they may contact the DPO for any issue related to processing their personal data.

Internal audit can educate management about potential risks and ways to manage risks in each area. Auditors can communicate relevant information about these risks via informal emails, a departmental newsletter, or meeting with management.

Assuring Compliance

As new policies and procedures become more mature, internal audit will need to perform regular compliance audits to determine the extent to which the organization is complying with GDPR. Auditors should focus on how the organization manages data to help strengthen privacy and security controls and ensure they are designed appropriately and operating effectively. Auditors will need to assure compliance with key aspects of the regulation and provide early warnings about problems.

Choice and Consent Under GDPR, organizations must allow users to choose how their personal data is used. Also, organizations must document and maintain consents and request parental authorization before collecting a child's data.

Legitimate Purpose To ensure data collection is lawful and necessary, organizations can collect only personal data that is needed to achieve the intended purpose. Reviewing and

handling requests for further processing, restricting requests for data related to criminal convictions, and documenting situations where the right to object does not apply are all important. Internal auditors can help reduce risk by sampling data collection mechanisms for compliance.

Limitations Organizations may keep data no longer than the period required to support the purposes for which it was collected, and they must erase an individual's personal data upon his or her request. GDPR permits organizations to retain data meant for archiving purposes in the public interest or for reasons of scientific or historical research.

Free Flow of Information and Legitimate Restriction


This principle includes protections for data transfers using legally binding agreements between public authorities, binding corporate rules, model clauses, and other mechanisms.

Third-party Vendor Management This principle ensures that organizations gather third-party/vendor guarantees of GDPR compliance along with proof that third parties have the required technical and organizational safeguards. The DPOs of the data controller—organizations or individuals that determine the purposes and means of processing data—must provide written authorizations to use a given processor.

Accountability GDPR's accountability principle provides a legal basis for processing personal data, establishes the DPO role, and informs citizens and residents of existing privacy rights and safeguards. In addition to overseeing the data protection strategy, the DPO must maintain contact with the supervisory authority and demonstrate compliance.

Internal auditors will need to periodically assess processes and controls for each of these principles to ensure they are designed and operating effectively. Auditors can review a sample of data transfer documentation to look for data that should not be transferred to another organization. They can run reports to look for data that is being kept longer than necessary and review available documentation for any exceptions.

A GDPR Audit Plan

To help the organization maintain compliance, internal audit should include independent GDPR assessments and compliance testing in the audit plan. It can raise executive and board awareness of GDPR noncompliance by highlighting poorly designed or missing controls. Finally, it can identify opportunities to audit common processes across departments. 

JAN HERTZBERG, CISA, CIPT, is a director at BKD in Chicago.



Trust Your Quality to the Experts

Leverage an External Quality Assessment in 2019

Build confidence with your stakeholders through a solid Quality Assurance and Improvement Program (QAIP). Look to IIA Quality Services' expert practitioners to provide:

- Insightful external quality assessment services.
- On-time solutions and successful practice suggestions based on extensive field experience.
- Enhanced credibility with a future-focused QAIP.

IIA Quality Services, LLC, provides you the tools, expertise, and services to support your QAIP. Learn more at www.theiia.org/Quality

Fraud Findings

BY MICHAEL MCSHEA + JEFFREY SARDELLI EDITED BY BRYANT RICHARDS

THE SLICE AND DICE FRAUD

A routine tax audit uncovers a \$1 million theft by a former employee with a criminal past.

Hanzo Enterprises was a global operation that produced fine cutlery for sophisticated consumers. While assisting government authorities during a routine tax audit, the Asia-Pacific controller, Jane O'Ren, discovered that company policies on the retention of support documentation for invoices was not being followed and details behind these invoices were raising red flags. O'Ren soon determined that the exceptions were related to invoices processed by the Okinawa location controller, Bill Tripp. However, Tripp had left the company during a downsizing process more than a year earlier.

O'Ren reached out to Tripp via email to ask about the invoices in question. Tripp responded almost immediately, apologized, and indicated he would take care of it. He later sent a payment of \$10,000. During the intervening time, O'Ren felt a knot forming in the pit

of her stomach and reached out to Hanzo's chief financial officer, Brad Gates, about what she'd found. Gates listened and determined legal and internal audit needed to be contacted. Beatrix Hales, Hanzo's new chief audit executive (CAE), was subsequently asked to meet with corporate counsel to discuss the situation.

After the meeting, a course of action was determined. The invoices at the Okinawa office needed to be reviewed for anomalies, discrepancies, support, and payment trails. Okinawa was a small operation and had not been included within the scope of U.S. Sarbanes-Oxley Act of 2002 controls testing. In fact, internal audit's focus had been primarily Sarbanes-Oxley testing at larger, in-scope locations, so it had not covered small operations globally.

The chief financial officer, internal audit, and corporate counsel selected

a third-party firm based on language skills necessary to review and translate documents. Hales made sure the external auditors were kept informed of the progress of the review as the discovery was close to the completion of the company's quarterly financials.

The review started with invoices from the Okinawa operation to ensure issues weren't prevalent in other locations. The invoice review soon spread to human resources (HR) and payroll once it revealed that Tripp had wide control on that side of the operation, as well. The scope of the issues grew exponentially as the review proceeded, but internal audit and the third-party team were able to determine the issues were confined to the Okinawa operation.

The fraud review identified numerous control deficiencies that allowed Tripp to carry out different methods of theft. In the small operation, Tripp was

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



Unlock the complexity of risk.

With the new COSO Enterprise Risk Management Certificate Program.

The complexity of enterprise risk has changed, new risks have emerged, and managing this has become everyone's responsibility. You can choose from our In-person or OnDemand formats to earn your COSO Enterprise Risk Management Certificate. You will learn the concepts and principles of the newly updated ERM Framework and be prepared to integrate the Framework into your organization's strategy-setting process to drive business performance.

Take control of your risk management strategy.
Enroll today: www.theiia.org/Training/ERM Cert.

COSO



TO COMMENT on this article,
EMAIL the author at michael.mcshea@theiaa.org

LESSONS LEARNED

- » Hanzo Enterprises didn't perform a fraud risk assessment, relying instead on its enterprise risk assessment, which allowed potential red-flag situations to go unaddressed.
- » Internal audit was structured to focus on Sarbanes-Oxley compliance, allowing attention to nonmaterial operations to slip. In essence, the third line of defense had governance failures.
- » Budget analyses were not performed at an appropriate level of detail to note excessive spending around renovations that were taking place at the subsidiary during Tripp's tenure, and to question such.
- » Tripp's fraudulent activity could have been detected earlier, or even prevented, if the review controls, such as invoice reviews, in place were executed appropriately.
- » Controls that were missing at the Okinawa location, including secondary review, segregation of duties, and exception reporting, were validated or implemented at all locations that were previously included within the scope of Sarbanes-Oxley controls testing.
- » Hanzo's detective controls over third-party service providers, such as its third-party payroll provider, did not include validation of transmitted files by an individual independent of the process, so Tripp was able to easily manipulate the system.
- » Detective controls also were not in place to ensure the approved payment register tied—in vendor name and payment amount—to the actual bank payment register, allowing Tripp to alter payment amounts and create vendors.
- » Due diligence efforts during the hiring process were insufficient given the importance of the controller position and its breadth of responsibility. Because Hanzo Enterprises did not conduct due diligence during the new-hire process, it didn't know that Tripp was a career criminal. Japan had strict privacy guidelines, but there were ways to ask the right questions to validate a candidate's responses with governing agencies and that was not done. Had Hanzo followed through and confirmed the candidate's background, it would have learned of Tripp's past.

the only person in charge of financial operations and HR. As such, he took advantage of his position in several ways.

As the Okinawa controller, Tripp was the only approver of invoices. The biweekly check run was sent as a file with supporting invoices to O'Ren for approval. Invoice review was not

of secondary review. Lastly, he manipulated the funds sent to the company's pension administrator by convincing her to not only return erroneous overpayments, but to return them to an account different than the source—his own personal account.

The fraud review determined that over two years, Tripp stole more than \$1 million. The efforts made by Hales to keep the audit committee and external auditors informed via status calls and check-ins kept worries at a minimum during the six-week investigation, and the interaction between legal and external audit helped

build cooperation and coordination. Legal found that Hanzo's insurance policy had provisions for loss due to fraud, so the company was able to file a claim for most of the losses.

Oddly, Tripp cooperated during the fraud review, answering questions and admitting guilt whenever presented with proof. Authorities arrested Tripp and his wife, who also had a criminal past, and confiscated cash, property, and vehicles. [la](#)

The interaction between legal and external audit helped build cooperation.

done at a level of precision to detect anomalies or even glaring fraudulent activity. Some paid invoices were for items Tripp purchased for his personal property or services provided.

Once the check run was approved, Tripp would log into the online bank account and change payment recipients. In many cases, payments were being sent to Tripp's credit card companies. He also easily created false vendors by editing the vendor master list. He was able to do both of these things without a requirement of secondary review.

Tripp also was in charge of the third-party payroll service interface and added extra funding to the file to get additional pay or expenses reimbursed without the requirement

MICHAEL MCSHEA, CIA, is director of internal audit and enterprise risk at KPMG in Boston.

JEFFREY SARDELLI, CIA, is director of internal audit at Brooks Automation in Chelmsford, Mass.

Arthur Piper

Illustration by Sandra Dionisi

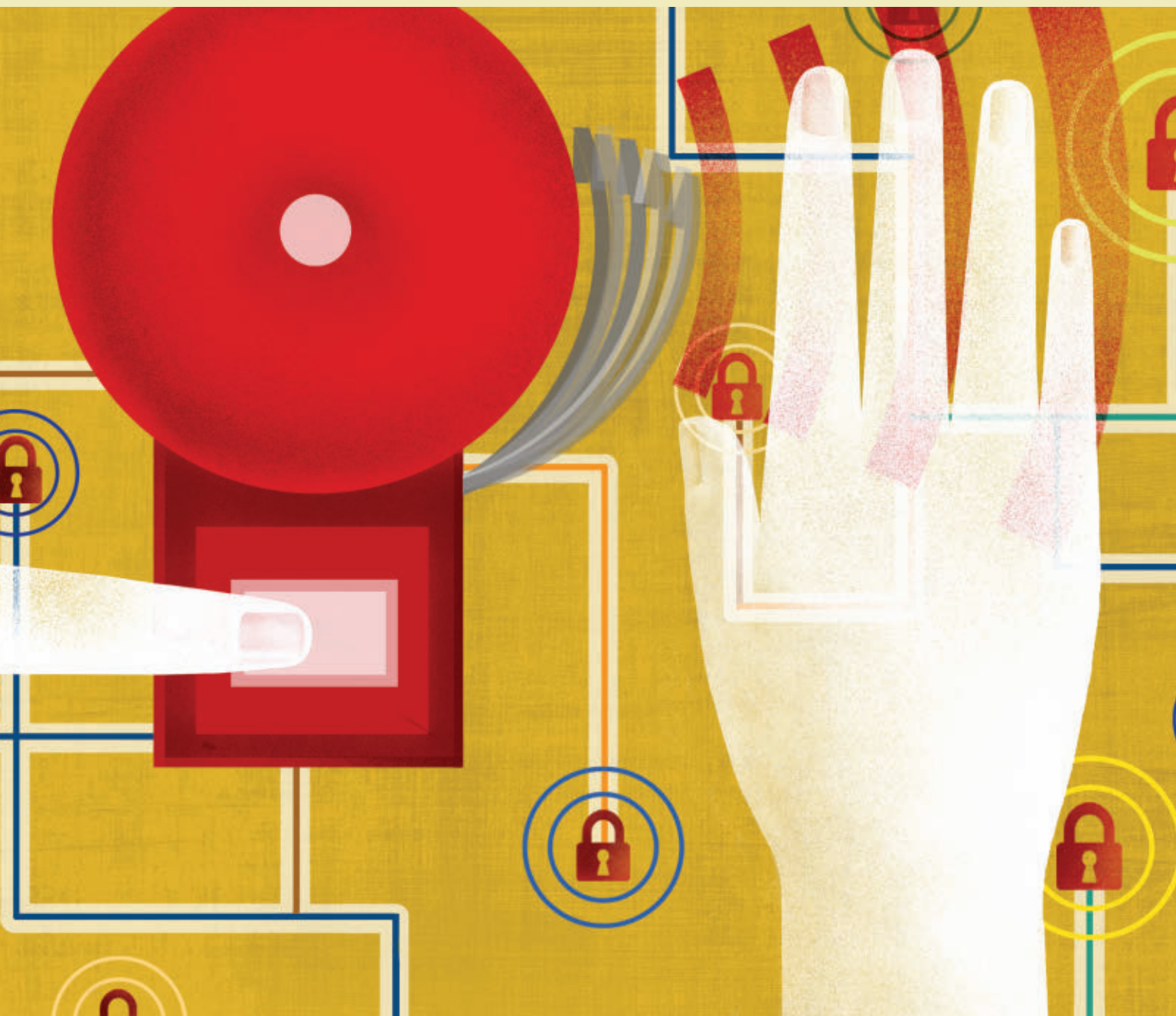
Victim organizations are paying a high price for ransomware attacks.

An illustration on the right side of the page. It features a white hand holding a white cloud. The background is a textured yellow. There are several red padlock icons, some of which are circled in blue or green. White lines resembling circuitry or data paths connect the padlocks and the hand. The overall theme is digital security and ransomware.

HELD HOSTAGE

The City of Atlanta is still trying to recover from the March 2018 SamSam ransomware attack that demanded \$51,000 in bitcoin. More than one-third of the city government's online systems were frozen, and staff were initially told not to turn on their computers in case the malware spread. Atlanta's public safety services, such as 911, police and fire rescue, as well as Hartsfield-Jackson Atlanta International Airport, were mostly unaffected.

When the attack occurred, the city was in the process of improving its cyber defenses following an internal audit report. Chief Audit Executive (CAE) Amanda Noble says it is too early to tell what lessons can be learned from the incident, but she says the fact that most emergency services stayed up and running suggests that the city had done a good job of segmenting its network before the attack—one of the audit recommendations.





Noble says about 600 of the city's 8,000 computers were affected. What struck her most immediately following the attack was the difficulty communicating throughout the city without email. Because local device hard drives had been potentially compromised, it was important to identify which ones were impacted before giving people access to their equipment.

"The day after we learned of the attack, building security was passing out notices asking staff not to use their computers," she says. While the City Auditor's Office had done a business continuity audit for the city, they had not done one for her own department. Auditors were locked out of their laptops for several days.

She says that organizations prioritize their most sensitive assets first—which is only natural—but they should be looking at how the entire enterprise can be affected during an attack, whether they have the resources in the short term to deal with those other areas or not. "It is worth remembering that Atlanta was not a uniquely vulnerable organization and that this was not a particularly sophisticated attack," she says. "Organizations should start approaching this by thinking in terms of not if this will happen, but when. Think about how to recover and about your communication plan."

TO PAY OR NOT?

Initial clean-up costs in the weeks following the Atlanta attack have been widely reported to have topped \$2.6 million, with more remediation efforts needed longer term. In June, Daphne Rackely, the city's interim chief information officer (CIO), requested an additional \$9.5 million for recovery efforts from city council as the city continues to find more problems with its systems, including the loss of more than a decade of legal documents and years of police dash-camera footage.

Ransomware is a specific type of malware that infects computers and mobile devices and, in doing so, restricts users' access to files. Attackers often threaten to permanently destroy data quickly unless a ransom is paid—or they increase the size of the demand incrementally each time a deadline for payment has been reached. The initial ransom demand can be small. So, with recovery effort amounts in Atlanta now topping \$14 million vs. the total reported ransomware demand of \$51,000, why not just pay?

Official government advice in the U.S. and U.K. is not to pay. "From the U.S. government perspective, we definitely discourage the payment of ransom," Neil Jenkins, former director of the U.S. Department of Homeland Security's Enterprise Performance Management Office, told the online magazine ZDNet last year. "From a national perspective ... paying ransom encourages the business model," he said. "The reason this has become such a popular thing to do is they're actually making money off of this."

Cyber defense experts tend to agree, even though the financial calculations may initially make payment attractive. "If you are a CEO losing \$100,000 a day and the ransom is \$300,000 in bitcoins, you could potentially get your money back in three days," Raj Rajamani, vice president of products at endpoint protection company SentinelOne in Mountain View, Calif., says. "But in the longer term, you are paying the attackers to become more sophisticated by helping them reinvest in building better attack technology."

Not only that, but paying ransom does not work in most cases. According to the SentinelOne Global Ransomware Report 2018, of the 45 percent of U.S. companies impacted by ransomware in 2017 that

paid at least once, only 26 percent got their systems back from the attackers. Seventy-three percent of those that paid were attacked again. For most, paying was a lose-lose scenario.

Most worrying, 44 percent of respondents claimed that ransoms have been paid without the involvement or sanction of IT and security teams. "Depending on how high up in the organization the employee is and what kind of data has been stolen, maybe he or she doesn't know how to react, sees it as their fault, and wants to hide it under the radar until the data can be retrieved," Rajamani explains. "The intention is understandable, but the reality is you are putting the rest of the organization at risk."

Organizations need to accept that people make mistakes and that if they become a victim of ransomware, they should feel free to raise their hand and tell someone immediately, Rajamani says. "These attacks are inevitable, so organizations should avoid creating a culture of fear where people feel they'll lose their jobs for coming forward with a problem," he adds.

MAKE ROUTINES ROUTINE

Organizations need to ensure they are paying close attention to basic IT routines. "The reason attackers are able to get in and get this kind of control over companies' systems is because the company has failed to do something it should have done," says Neil Frieser, senior vice president of internal audit at telecommunications company Frontier Communications in Norwalk, Conn. And internal audit's role is to understand whether basic security policies and routines are in place and have been followed.

"Failure to patch vulnerabilities in a timely way is No. 1 on the list of cybersecurity issues," Frieser says. Manufacturers regularly update their hardware and software with patches

41% of organizations see themselves as likely targets of a ransomware attack in the next 12 months, according to RSM's U.S. Middle Market Business Index Cyber Security Report.



“Avoid creating a culture of fear where people feel they'll lose their jobs for coming forward with a problem.”

Raj Rajamani



“Organizations should start approaching this by thinking in terms of not if this will happen, but when.”

Amanda Noble

that help to protect those devices and programs from attack via vulnerabilities. Unlike consumers, who can generally download the latest updates with the click of a button, companies have to ensure that when they apply a patch to a particular system, it will still work as intended on the network. Frieser says it is critical for someone on the network infrastructure team to ensure that patching happens timely across the organization.

“I'm a big believer in the concept that routine things need to be done routinely and patch management falls into that,” he says. “It has to be a priority because it only takes one vulnerability to create potentially serious problems.”

During Frontier's annual cybersecurity audit, Frieser's team looks to see whether the business has any exposures on patching that are known about, but not yet dealt with. They also look at the process. “Just because there are no outstanding issues does not mean that the patching process is good,” he says. “Someone may have just done the patch updates because they knew the auditors were coming.”

The other major issue for Frieser is access reviews. Auditors should be periodically looking at all of the users in key systems. Generic IDs and passwords should be weeded out. Key questions to consider, he says, are whether there are IDs that have not been used for long periods or IDs that are associated with people who are no longer with the company or with people who have changed roles and no longer need the same access levels.

“If you have a generic ID for administrator, with ‘admin’ set as the password—and where it's shared—it is crazy to have that in your company's infrastructure,” Frieser says. Privileged access is a critical area for auditors to focus on, because hackers who get into the system can begin to shut things down associated with that access

point—and potentially hold the business for ransom.

While organizations and auditors are generally aware of both of these key areas, they need to be constantly monitored. “Issues often arise due to laziness,” he says. “For example, someone might set up a generic admin ID and password in the throes of implementation, which they intend to change, but then forget about it and it becomes a vulnerability.”

THE PEOPLE FACTOR

Even with good controls over patch management and access rights, organizations can still be at risk of a ransomware attack.

“A lot of technical security has been commoditized to the extent that it is hard to switch off the safety measures in the software where it has been properly patched,” says Edward Wolton, deputy CEO at the London-based security consultancy Templar Executives. “People are often the greatest vulnerability, especially if they do not know what to do in the case of an attack.” Organizations need to put in place training for all personnel and have a well-circulated policy on what to do in case of a security breach.

BOARDS ARE PAYING ATTENTION

One of the more fortunate side effects of recent attacks, such as that on the City of Atlanta and last year's WannaCry that affected the U.K.'s National Health Service (NHS) among many others, is that it has brought the issue into the boardroom. In May 2017, WannaCry caused the NHS to cancel 20,000 hospital appointments and affected 80 of its 236 Trusts, which are responsible for running the organization's health services—everything from hospitals to ambulance services—as well as hitting 200,000 computers in at least 100 countries. An April 2018 report by the U.K. government's

SIX STEPS TO BETTER SECURITY

As ransomware is on the rise, Michael Lisenby, managing partner at Rausch Advisory Services LLC in Atlanta, gives advice for minimizing the odds of an organization falling victim to an attack.

1. Establish security awareness campaigns that stress the avoidance of clicking on links and attachments in email from unknown senders. That could include, for example, the technology department running phishing campaigns, which internal audit evaluates in terms of the effectiveness of the organization's training and education processes and to identify frequent offenders.
2. Ensure antivirus software is installed and is up-to-date across all endpoints within the business. Antivirus software on its own is unlikely to be enough, so the organization may also evaluate next generation antivirus programs that include endpoint protection. This can look for ransomware attempts and provide IT with the ability to monitor attacks to stop them from spreading. Internal audit should be looking at the cyber defense IT road map and strategy and evaluate configurations.
3. Use content scanning and filtering on mail servers. Inbound emails should be scanned for known threats and should block any attachments that could pose a threat. While spam protection should identify and block a lot of these attacks, advanced threat protection tools should be inserted into the mail flow, which will look for and quarantine unsafe messages that may contain malware, for instance. It can also scan URLs to ensure phishing attachments are identified and protected.
4. Restrict users' ability (permissions) to install and run unwanted software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
5. If the data is backed up to an external storage device, remove the device after backup so that if ransomware does infect the computer, it won't be able to spread to the device. Where organizations depend on cloud backup, ensure there is off-site replication of essential data.
6. Apply a patch management system, making sure all desktop clients are fully patched. Ensure the system is patching commonly exploited third-party software – such as Java and Adobe Flash – which will prevent many of these types of attacks from being successful.

House of Commons Committee of Public Accounts said the attack most likely exploited unpatched vulnerabilities in Windows XP—even though the NHS had been warned about the dangers repeatedly since 2014.

Wolton says media coverage of the NHS attack in the U.K. suddenly made organizations and their boards pay attention and has, in some ways, made ransomware less of a threat due to raised awareness. It also has provided CAEs with an opportunity

to advocate for cybersecurity to be moved further up on the agenda. "Traditionally, responsibility for IT security has been pushed downstairs by the board to the CIO," Wolton says. While many CAEs are not on the board, he advises them to ensure there is board-level sponsorship for the issue—and that the sponsor really understands the nature of the threat to the organization.

"While it is changing rapidly, too many businesses fail to have a

senior-level sponsor who understands the risks and the level of network and governance controls needed to minimize the threat," he says. In devising a policy on ransomware that spells out the organization's response, boards will need to decide on the level of risk they are prepared to accept and review their backup policies and procedures. If they decide that in certain circumstances they will pay the ransom, they will also need a cryptocurrency policy and capability.

Ransomware detection increased 350% from 2016 and accounted for 7% of global malware in 2017, according to NTT Global Security's 2018 Global Threat Intelligence Report.

Internal audit has an opportunity to educate the board and expand its influence. From a board perspective, internal audit should be working with boards to develop reporting metrics and monitor protocols to evaluate the organization's cyber defenses and, in turn, help mitigate the risk of future attacks.

RECOVERY FROM AN ATTACK

Wolton says organizations have become a victim of progress when it comes to backing up critical information. Twenty years ago, for example, most businesses had separate monthly, weekly, and daily backups, with the first two types being stored off-site. Today, many rely on continuous cloud-style backups. With this newer technology, it can be difficult to wind the clock back after a ransomware attack and identify when the system first became infected. That is why a robust backup policy and detection capabilities are crucial.

In fact, while awareness of ransomware threats is rising, many organizations are not looking at the problem from a recovery perspective. "A lot of CAEs and CIOs are now doing risk assessments on ransomware, but fewer are considering it from a disaster recovery perspective," says Michael Lisenby, managing partner at Rausch Advisory Services LLC in Atlanta. Lisenby says CAEs should be approaching the problem from the perspectives of prevention, detection, removal, and recovery.


"That entails conducting tabletop scenarios with all those who are likely to be involved in dealing with a ransomware crisis," he says. The more the team members have practiced the routine, the less likely they will be surprised by their vulnerabilities. In the Atlanta and NHS attacks, for example, the reality of having to communicate without emails had not been fully tested. Lisenby says it is worth the team considering the threats to their operations both from a business

and an IT perspective to get a full view of the enterprisewide nature of the risks. Because the entire organization is affected, he says the heads of legal, finance, human resources, IT, risk, internal audit, and others should be involved—as should regulators, where appropriate.

"This is not a once-in-a-lifetime exercise, it has to be done annually," Lisenby says. That is because the nature of ransomware attacks and their impact on an organization are constantly changing. For example, Internet of Things (IoT) devices are opening up new and unlikely vulnerabilities. "I know of a casino where player data was stolen from its systems," he says. The culprit? A smart thermostat in an aquarium on the shop floor.

"There are products out there that enable you to scan to see if IoT devices have been added, and you can make sure they are segmented from the network and access of least privilege is associated with them," Lisenby says. "But only if you keep on top of the issue and make sure you have the right routines in place."

BEST TO BE PREPARED

Ransomware attacks are simple and effective. Organizations need only one point of weakness to be vulnerable, so, as Noble says, it is more a case of when it happens, rather than if it will. Having a proactive approach to the problem with regular and effective training for staff across the entity is a good place to start. But organizations also need to have well-tested plans for when an attack strikes successfully, with effective data protection systems in place and business continuity routines that work. 

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



Too many businesses fail to have a senior-level sponsor who understands the risks."

Edward Wolton



Fewer [CAEs and CIOs] are considering [ransomware] from a recovery perspective."

Michael Lisenby

PULLING STRINGS

Russell A. Jackson

Detection is fast and effective for a criminal trying to access a company's data and assets, because it's easier to trick people than to hack their hardware or break into their offices. Well-intentioned employees will offer account numbers, volunteer passwords, and even open locked security doors if the request seems reasonable or the threat seems real—or if the stranger seeking physical access is a decent actor with an adequate disguise.

Emails with interesting content, infuriating social media messages, bogus package deliveries, and phone calls with tantalizing offers—four basic forms of social engineering—seem innocuous, and a waste of company time. But they're among the biggest risks organizations now face. When businesses catch on to current tricks and mount new defenses, the perpetrators change the rules, so flexibility and virtually constant vigilance are necessary—and human resources executives, IT managers, and physical plant security personnel need to be involved. For internal auditors, the shape-shifting challenges of social engineering demand assessment and advice on evolving threats and a diverse, integrated, and coordinated response.

PHOTOGRAPH: ANDREY POPOV / SHUTTERSTOCK.COM; BACKGROUND: SUNSPIRE / SHUTTERSTOCK.COM



High-level hackers are using social engineering tactics to manipulate employees into giving up vital information.



EVOLVING TACTICS

One of the things that's changed over time is that now "the individuals doing this are highly sophisticated," says Kimberly Hagara, vice president, audit services, at the University of Texas Medical Branch (UTMB) in Galveston, part of the University of Texas (UT) System. "In the early days, you received emails asking you to contact some foreign government," she says—usually to "help someone out" or to claim a cash windfall. "Now the tactics are much more trust-based," she adds. "Getting into an organization or a system relies more on human interaction."

The No. 1 way to get into an organization's system is by spear phishing, mainly because it's global in reach and free. "Or with phone pretexting, you can simply talk to anyone on the phone and get instant compliance from the victims, often getting them to take the time to follow instructions," says Kevin Mitnick, CEO at Mitnick Security Consulting in Las Vegas. The hacker gains access when the recipient clicks on a link in an email, a button on a website, or opens an attachment, he adds.

Phishing succeeds when the culprit convinces the recipient there's something at stake if he or she doesn't comply—even if the fake invoice attachment comes from



a vendor the organization doesn't do business with. Mitnick, who was once the U.S. Federal Bureau of Investigation's Most Wanted Hacker for hacking into 40 companies, explains that an employee who's just curious may not stop to "think critically about whether the email makes sense." And then it's too late. Organizations can install email filters to help identify questionable content but they may find that hackers can bypass them. "When you fix one thing," he says, "they'll attack another."

Social media can present effective social engineering targets, Mitnick says. "When organizations give employees permission to use social media on company equipment, those who haven't been trained could fall for LinkedIn attacks, for example," he explains, which can be messages encouraging them to click on a link for a business opportunity. "The link redirects the victim to a malicious website," he says. "If an attack like that is well-targeted, it will probably work. If it's sent to a lot of people, it's less likely to." That's because word gets around fast, and then the jig is up.

Simply picking up the phone works, as well. In fact, "phone pretexting has a high level of success depending on the hacker's skill set," Mitnick says. "People need to understand that social engineering isn't just a phishing problem. It's deception." Indeed. Social engineering isn't just duping someone online—it's also used to gain access to physical premises. An attack like that is a much higher risk for the social engineer, though, which is another reason perpetrators focus on email and phone scams.

PHYSICAL RISK

Physical access is sometimes breached, too. Many organizations maintain multiple buildings—in the UTMB's case, that includes offices, classrooms, health-care services, and research facilities—with varying types and levels of security. Says Hagara: "We look at

WHAT IS SOCIAL ENGINEERING?

Social engineering often starts with recon: Criminals get an idea of an organization's internal operations and corporate lingo first, then target security guards or receptionists, who offer access rather than information. They then use various forms of deception to trick employees into volunteering sensitive information or responding to bogus email enticements, often exposing the organization's entire IT infrastructure to attack.

Social engineering is such an effective tactic and comes in many forms:

- » **Baiting.** Placing a malware-infected physical device somewhere it's sure to be noticed; when it's loaded onto another computer, the malware is installed (such as a USB flash drive).
- » **Phishing.** Sending fake email, often claiming it's from a trusted source.
- » **Pretexting.** Lying to gain access to privileged data, such as pretending to need personal data to confirm someone's identity.
- » **Quid pro quo.** The social engineer pretends to provide something—claiming to be a return call from tech support, for example—in exchange for the target's information.
- » **Scareware.** Tricks the victim into thinking a computer is infected and offers a solution to the problem that actually installs malware.
- » **Spearm phishing.** Precision phishing, tailored to a specific individual or organization.
- » **Tailgating or piggybacking.** Following someone into a secure building, assuming that person is willing to hold the door open.
- » **Vishing.** Voice phishing; social engineering over the phone.
- » **Water-holing.** The attacker targets a specific person or people by infecting websites they're known to frequent.

physical security from a risk perspective, focusing on which buildings hold sensitive information or access to other information, and what the physical security requirements are."

One requirement, she says, is that "we have to remain an open campus. We have a lot of people coming and going, including patients who come to campus, colleagues from other institutions, and vendors." The UTMB conducts an awareness campaign around wearing ID badges, and stresses that someone who suspects something shouldn't be afraid to speak up.

Still, she adds, people want to help, and they don't want to be rude, asking people to justify what they're doing. But social engineering—which may start

with someone looking over a shoulder to gather information and then develop into someone pretending to carry a heavy box while asking, "Could you hold that door for me?"—requires a tougher stance. "Even though we're a 24/7 operation," Hagara points out, "is a printer really going to be delivered at 10:30 p.m.?" In those cases, demanding identification is OK.

FOOL ME ONCE

When Mitnick's firm starts a social engineering training engagement, his team members use phone calls, spear phishing, and phone pretexting pretending to be people they're not, and they can "always convince the client to do things" they want them to do. He

Phishing and financial pretexting represent 93% of all breaches investigated— with email being the main entry point (96%), according to Verizon’s 2018 Data Breach Investigations Report.

adds that social engineering is a problem that needs to be addressed because there’s too much at stake to ignore it.

“Most social engineering schemes I’ve seen are individuals giving up confidential system identification or passwords,” says Kenneth Pyzik, vice president, audit professional practices, at Western Alliance Bancorp. in Las Vegas. That’s often the entry point the hackers want, so they can implant a Trojan horse or other piece of malware for later data mining exploits. Initial entry may not be detected, he adds, and the longer the breach remains unnoticed, “the more brazen the attack becomes to get at any kind of valuable information.”

In his experience, the perpetrator’s target is usually customers’ credit card numbers, Social Security numbers, and driver’s license numbers “that can be used for financial identify theft or some other illegal gain,” Pyzik says. And they don’t want just the data from the person who answers the phone or opens the email. “The real asset is customer lists and customer data,” he says. “The mother lode is not duping a single person for a single credit card number, it’s getting to the customer file for thousands of them.”

Risks for Hagara include researchers’ intellectual property, patients’ clinical and financial information, UT’s financial data, and sensitive details about students and employees. For example, payroll information includes tax identification and Social Security numbers, she explains. And simple email hacks and bogus pizza deliveries often aren’t a school’s biggest worry, Pyzik adds. “In addition to financial hacks to commercial enterprises,” he says, “if the entity doesn’t have valuable customer data, then another objective is to plant malware that can later lock system files and demand ransom” (see “Held Hostage” on page 28).

Small and medium-sized enterprises (SMEs) don’t escape social

engineers’ attention, either. “They’re regularly targeted,” Mitnick points out. SMEs often don’t have the funds for IT staff and security, so they’re low-hanging fruit—a perpetrator doesn’t have to work as hard, and a phishing expedition is very likely to work.

“Generally, employees want to do good—they want to help others get their jobs done so they can go back to getting their work done,” says David Bryan, associate partner and global leader of technology for IBM’s X-Force Red security testing service in Minneapolis. “Email phishing can’t be stopped, but a targeted attack can be prevented with training and testing to determine if the training was effective.” Mitnick advocates combining user education and training videos. “When you know what the scams are, you’re less likely to fall for them,” he says.

WHERE TO START

When the C-suite asks for advice on addressing social engineering, “the thought processes internal audit needs to emphasize are education, simulated phishing, and a layered security approach,” Mitnick advises. “And make sure to recommend that the enterprise maintain a process for mitigating risk when something is infected”—whether that’s determining internally if the threat is “domestic or something in the wild” or outsourcing the investigation.

Also, Mitnick says, internal audit should recommend that organizations maintain a social engineering instant response program to mitigate an attack. Often, a third-party sets up a system that sends an alert when an employee clicks on a suspicious email icon, then advises the organization and helps it measure people’s progress on compliance. He also suggests regular penetration testing to see if security controls are holding up.

The internal audit department can recommend those programs



“We look at physical security from a risk perspective... and what the physical security requirements are.”

Kimberly Hagara



“Social engineering isn’t just a phishing problem. It’s deception.”

Kevin Mitnick



When you know what the scams are, you're less likely to fall for them."

David Bryan



The whole company is at risk when employees are lax."

Kenneth Pyzik

PREVENTION AND DETECTION TIPS

Experts offer advice on how to keep attacks from happening, or catching them early if they do.

- » **Start with the basics.** Passwords should not be shared among employees for any reason, says David Bryan, associate partner and global leader of technology for IBM's X-Force Red security testing service. "If you make that a part of the corporate culture, employees will be less likely to freely give passwords to outside persons." Kenneth Pyzik, vice president, audit professional practices, at Western Alliance Bancorp. in Las Vegas, emphasizes: Don't forget automated spam filters on email and an easy-to-use phishing icon to quickly report suspicious correspondence.
- » **Include everybody.** All system users should be subject to the same email precautions and restrictions, Pyzik says. "There's no executive privilege," he adds. "Executives can sometimes be the weakest link."
- » **Practice beating perpetrators at their own game.** "Attack your employees like the bad guys do," Kevin Mitnick, CEO at Mitnick Security Consulting in Las Vegas, advises. There are email phishing platforms that "train and inoculate" staff members.
- » **Don't make matters worse.** When testing employees' vulnerability to social engineering scams, make sure they know in advance that they're being tested, so employee morale isn't ruined. Explain that added security helps them, too—when they buy movie tickets, say, and pay with a personal credit card on the company computer. "You want to be transparent," Mitnick adds. "You can't make testing completely transparent, but make it part of everybody's job duties to be knowledgeable about how scams are carried out."
- » **Be fair.** "You can't punish employees for making human mistakes," Mitnick says. He prefers the carrot to the stick, such as "an educational message saying that you made a mistake, and that you need to stop and think before you click."
- » **Keep sending the same message.** Raising awareness of social engineering scams may not keep employees from falling for them. Measure how employees perform at a baseline level, then track testing results to see who needs special attention, such as more training videos for additional education.
- » **Don't stop short of true enforcement for repeat offenders.** Some institutions conduct random testing and then let supervisors know when their employees have failed the tests. "Education is then required, and repeat offenders should be reprimanded," Pyzik says.
- » **Focus on esprit de corps.** "Protecting the network and protecting the company's confidential information needs to be part of every employee's job," Pyzik says. Mitnick adds, "Build a human firewall. Make sure everybody shares the common goal of increasing security for all."
- » **Use advanced technology.** "You want a good endpoint security product that works well at detecting threats," Mitnick says. Depending on the sophistication of the perpetrator, you might catch ransomware or other malware before it can do much harm.

76% of organizations experienced phishing attacks in 2017, according to surveyed information security professionals in Wombat Security's State of the Phish Report 2018.


and policies, Pyzik says, and can periodically audit the information security department to make sure it's addressing social engineering risk as a priority. The UTMB regularly runs scenarios to help teach its employees about social engineering techniques and technology solutions. "We do a lot to try to protect our system before a perpetrator gets into the network," Hargara says. "That includes quarantining email that appears suspicious or malicious. And we monitor foreign access to our network, among a variety of other technical controls that supplement administrative, individual, and behavioral controls."

Technological controls can be assessed by internal audit, she notes, and her shop does so periodically. The information security officer at

the UTMB "does annual third-party penetration testing scenarios and walk-throughs," she adds, to provide a level of assurance that controls are operating as intended.

TRUST AND WHAT'S AT STAKE

During a recent penetration test conducted at the UTMB, one employee who knew about the test in advance said, "You won't be able to get past me," Hargara says. But during the testing process, that employee clicked on the bait, and could have given up sensitive information. What worked? The email had a professional look, and the information it purported to contain was close to a real-life scenario, like a press release the employee would normally respond to. "It looked right and it felt right," she says.

"The incident exposed a vulnerability," Hargara adds, "and that helped us understand, from an employee standpoint, where the greater risk was and how we could further protect sensitive information. Humans are incredibly trustful." That's why, she emphasizes, defending against social engineering is really about education and awareness training of the risks for the organization, employees, and students. Make sure, Pyzik says, that employees understand what's at stake. "The whole company is at risk when employees are lax," he says. "One mistake can end up costing a company millions of dollars and many peoples' jobs." 

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

Emerging Leaders Forum: Young Professionals on the Rise

OCT. 21, 2018 / LAS VEGAS, NV

Develop the skills necessary to be an outstanding, valued practitioner and leader in the internal audit global landscape.

Register today for the Emerging Leaders Forum at www.theiia.org/EmergingLeadersForum.

If also attending All Star, save \$100. Contact Customer Relations at +1-407-937-1111 or CustomerRelations@theiia.org to register.



2018-1121

Deloitte.



The innovation imperative

Forging internal audit's path
to the future

Internal Audit groups most engaged in innovation are those most likely to have strong organizational impact and influence. That's just one of the insights from our second global survey of internal audit leaders. Find out what internal audit can do to stay ahead of disruption and forge a path to the future.

Learn more at www.deloitte.com/globalcaesurvey

Internal Audit and the BLOCKCHAIN

There's more to blockchain than bitcoin, and auditors have much to learn about how it works.

W

hile cryptocurrencies like bitcoin have received the attention of investors and regulators, it is their underlying technology—the blockchain—that has the greatest potential to disrupt and reshape traditional business and financial processes and infrastructure. The excitement centers on blockchain's ability to create a distributed ledger of transactions that is secure and can be publicly available in real time.

With blockchains, transactions can be logged, viewed, monitored, verified, and analyzed. For example, instead of a financial institution acting as an intermediary for the transactions, the blockchain technology, itself, takes on the role of a financial middleman, reducing or possibly eliminating many of the transaction fees and processing delays. Blockchains can enable automakers to track a vehicle from pre-production to sale. Similarly, the food industry is investing in blockchains as

**Lorraine Lee
Kirk Fiedler
Richard Mautz**

a possible solution for traceability and food safety. With blockchains gaining ground in a host of industries, internal auditors need to understand the technology and its audit implications.

BLOCKCHAIN BASICS

Blockchain technology has been touted as a potential game-changer for businesses because of its ability to verify a transaction without a trusted third party. Blockchains and bitcoins are closely intertwined, because bitcoins represent an active, commercial application of a blockchain.

In the bitcoin infrastructure, the blockchain is a continuously growing log of currency transactions that is shared and stored on multiple nodes in a network. Blockchains take advantage of three technology concepts to

shared information. Each node in the P2P blockchain network participates in maintaining the security and accuracy of the information. Each node can store a complete copy of the blockchain—as is in the case of a bitcoin blockchain—or use other types of decentralized storage technologies to manage the data associated with the blockchain.

Public Key Cryptography Blockchain verifies digital identity using public key cryptography. For example, in the bitcoin blockchain, the digital wallets use public key cryptography to send and receive bitcoins securely. This type of cryptographic system uses a pair of public and private keys, where the public key is freely available and the private key is known only to the key owner. The owner uses both a private key and a public key to send and receive messages. Public key cryptography can authenticate a message, where a public key is required to view a message that was encrypted with the corresponding private key. Because the message can only be decrypted with its matching public key, the message is authenticated as created by the owner of the private key. Likewise, a person can use the owner's public key to encrypt a private message, which can only be decrypted by the owner with his or her matching private key.

Transaction Verification Methodology A methodology must be in place to establish the legitimacy of a transaction within the recording node. The specific transaction verification methodology can vary across different implementations of blockchains. Because blockchain exists on a distributed network of computers maintaining shared information, trust is enabled by the collective record keeping by all nodes in the network. New blocks are added through verified nodes that ensure the integrity of values within a blockchain and

Because blockchain exists on a distributed network of computers, trust is enabled by the collective record keeping by all nodes in the network.

create a robust, secure, and potentially anonymous distributed data structure: peer-to-peer networking, public key cryptography, and transaction verification methodologies.

Peer-to-Peer Networking A simple peer-to-peer (P2P) network consists of two or more computer systems connected together to share resources without the use of a separate server computer. P2P networking enables file-sharing services such as Napster, the pioneering music sharing service, and Skype, the internet telecommunications network. Based on P2P networking, a blockchain consists of a distributed network of computer nodes that maintain

Global spending on blockchain is expected to double to **\$2.1 billion** this year and is estimated to be \$9.7 billion in 2021, IDC's Worldwide Semiannual Blockchain Spending Guide reports.

THE BLOCKCHAIN AUDIT

Internal auditors and the technology specialists they work with need to thoroughly understand how blockchains work and the risks involved with them. Auditors will be involved in auditing the technology associated with blockchains, as well as retrieving transactions from them. Moreover, because the software needed to maintain transactions in a blockchain is complex, auditors must provide assurance related to the system's control environment. Their priority should be reviewing the robustness of computer nodes that are part of a blockchain network.

In addition, auditors should focus on testing controls directly related to blockchains. These controls include:

- » Testing the availability of blockchain data from different nodes in the network.
- » Ensuring the accuracy, completeness, and consistency of the data elements that are stored within the blocks.
- » Verifying the identicalness of data obtained from different nodes in the network.
- » For private blockchains, testing access controls to ensure that only authorized personnel can view or update the blockchain.
- » Testing the process for adding new blocks to the blockchain.
- » Verifying the immutability of the blockchain to provide assurance that attempts to modify previously approved blocks are unsuccessful.

prevent the tampering of values within a verified block.

For example, the bitcoin blockchain uses proof-of-work to verify transactions and to add a new block of transactions to the blockchain. This method is known as the bitcoin mining process and involves bitcoin miners competing to solve a computational-intensive problem. Solving this problem entails finding a hash number with special properties dependent on the contents of a specific block of bitcoin transactions in the blockchain. The hash number is used to validate the data of the current block and prevent the tampering of data in previously validated blocks. The first miner to successfully identify a valid hash number for the block is rewarded, and the block is then added to the blockchain.

NEW LEDGERS AND CONTRACTS

Blockchains are closely associated with two technical innovations: distributed ledgers and smart contracts. A blockchain is a type of distributed ledger,

which is a record of transactions maintained across different locations without the need of a central authority to maintain transaction integrity. Unlike a centralized ledger, a distributed ledger does not rely on a single, authoritative version. Instead, copies of the ledger are stored on multiple nodes, and each copy is complete and valid. The responsibility for maintaining the data integrity of the ledger is shared among the nodes through the consensus-building, verification process.

While a blockchain consists of a sequence or chain of blocks of transaction records, a distributed ledger does not necessarily require a chain structure. Additionally, distributed ledgers do not necessarily require proof-of-work for transaction verification and may use a different verification methodology.

Whereas a distributed ledger is associated with recording transactions, a smart contract is a method of establishing contracts. A smart contract is used to digitally establish a business relationship, including identifying



the terms of an agreement, executing the agreed-upon terms, and verifying fulfillment of the agreement. Because a smart contract is typically implemented with blockchains, the contract cannot be modified or tampered with after it has been accepted into the blockchain. Additionally, every node in the distributed network validates the transactions associated with the contract. Smart contracts have been used to track items within a supply chain and to improve loan processing and insurance claim processing.

FIVE RECOMMENDATIONS FOR AUDITORS

One of internal audit's roles is verifying and reconciling transactions (see "The Blockchain Audit" on page 43). Because transaction processing is at the core of blockchains, auditors can do five things to better understand the technology:

1 Understand that blockchains are a form of transaction-based data storage. The blockchain is a continuously growing link of blocks that are validated and secured through public key cryptography. In addition to transaction data, each block contains a link to the previous block in the chain, as well as a time stamp on when the block was created. Just as internal auditors have adapted their skills to retrieve data from enterprise resource planning and cloud computing systems, they will need to learn data retrieval methods to assess the data and controls of blockchains. For example, if an organization is using a blockchain to manage its supply chain, the internal auditor should be able to retrieve individual transactions from the blockchain to verify the accuracy and completeness of the blockchain.

2 Explore the implications to audit. Blockchains can have implications for developing

appropriate audit procedures. With blockchains, a complete copy of the data is accessible at every node, enabling auditors to test the entire population of transactions instead of relying on sampling. During completeness testing, auditors should be able to trace transactions from the blockchain to the financial statements. For occurrence testing, the auditor may perform vouching procedures to verify that values on the financial statement are directly associated with transactions in the blockchain. In addition, a combination of tools related to data analytics and artificial intelligence could assist with fraud detection through pattern recognition across the entire transaction population. This capability could shift the focus of auditor responsibility toward the planning and investigation of anomalies.

3 Explore the implications to financial services. The financial services sector is actively identifying areas beyond bitcoin with blockchain implications. For example, financial institutions are exploring the use of blockchains and distributed ledgers for payment, clearing, and settlement activities. Blockchains could also be used as a platform for stock trading, which could minimize the need for stock brokers and a centralized stock exchange. Additionally, blockchains can manage the process of issuing shares of a company or taking a company public. In late 2015, Nasdaq announced that its Linq blockchain ledger technology was used to issue shares of a company to a private investor. Finally, blockchain technology is being used as a platform for managing shareholder proxy services such as proxy voting.

4 Explore the implications to supply chains. Supply chain management is a promising area for blockchain usage because

Venture capitalists **invested** more than **\$1 billion** in blockchain **start-up** companies in 2017, according to research firm EB Insights.

blockchains can provide insights into the visibility and traceability of an item. This is particularly useful in cases where an item passes through numerous parties before it reaches the final customer. For example, in December 2017, IBM and Walmart announced they were participating in a blockchain alliance in China to enhance food tracking, traceability, and safety. Another example is the automotive supply chain, where blockchains can be used to track the transactions associated with a specific vehicle, such as production, ownership, financing, registration, insurance, and maintenance. As most organizations are part of some type of supply chain, auditors should be aware of possible internal projects related to blockchains for tracking information or physical assets. Auditors should seek opportunities to participate in prototype efforts to develop their technology skills. Such skills will benefit them when it is time to audit blockchain projects.

5 Embrace the reality that new technology will continuously change the skills of auditors.


Internal auditors may need additional training to understand the technology and its implications, and internal audit departments may need to add expertise with these skills. This is especially important for internal auditors in organizations that are already implementing blockchain projects, as auditors may be tasked with evaluating the data controls associated with blockchains. With the conceptual understanding that blockchains represent a new type of data structure for storing and accessing information, traditional application and data controls related to input, processing, and output will still apply, albeit with certain adaptations. For example, a standard application control is that output reports

should be protected from unauthorized disclosure. With all transactions potentially accessible on the blockchain, internal auditors may need to recommend additional controls related specifically to authorization, privacy, and confidentiality.

CONTROLLING THE CHAIN

Blockchain's potential to revolutionize transaction processing rests with its ability to create a secure, trusted, distributed ledger of transactions that can be accessed without the overhead of a middleman or a centralized authority.

Internal auditors may need to recommend additional controls related specifically to authentication, privacy, and confidentiality.

Internal auditors will be responsible for recommending controls associated with organizational processes that use blockchains, including the acquisition, protection, delivery, and enhancement of the information assets stored within them. Moreover, traditional IT controls related to security, availability, processing integrity, privacy, and confidentiality will continue to apply. Internal auditors must understand the technical details of blockchains to recommend adaptations of traditional IT controls as their organizations adopt new blockchain-based innovations. 

LORRAINE LEE, PHD, CPA, is an associate professor of accounting at the University of North Carolina-Wilmington.

KIRK FIEDLER, PHD, CPA, is an associate professor at the University of South Carolina in Columbia.

RICHARD MAUTZ is a doctoral student at the University of Georgia in Athens.

Anyone who has been exposed to employee fraud knows how unsettling it can be to learn that someone known and trusted has betrayed co-workers and the organization itself. Shocked employees wander the office halls, whispering to each other, “I would never have suspected him of doing something like that.”

And the perpetrator may, indeed, be a likable, friendly person who maintained cordial relationships with colleagues. Even good people occasionally stumble.

Internal auditors are responsible for understanding and assessing the red flags that may indicate that such a stumble is being considered or has already occurred. Proactive recognition and response can go a long way toward protecting the enterprise from the financial and reputational damage a successful fraud can create.

HOLDING THE LINE

Fraud represents one of the many risks associated with an unhealthy culture (see “It Starts With Culture” on page 49), and one that internal audit can address directly in its capacity

Internal auditors must be alert to the red flags of fraud, even when they point to the organization’s most trusted employees.

The ones
 you **LEAST**
 suspect

Richard F. Chambers and Deanna F. Sullivan



as the third line of defense. The first line, management, sets, communicates, and models desired values and conduct. The second line, oversight functions such as an ethics office, monitors risks related to employee conduct and compliance with policies and procedures. Internal audit assesses various functions and lines of business and determines whether values and behaviors that drive strategy and good performance are embedded in the organization.

Although this role may be clear to internal auditors, how to approach it may be less apparent. The job can be tackled in many ways, but two objectives should remain paramount: understanding behaviors (red flags) associated

fraud. When people faced with a non-sharable financial problem realize they can alleviate that problem through violation of a position of financial trust, and are able to convince themselves that their dishonest actions don't run afoul of their personal codes of conduct, they make a transition Cressey describes as going from "trusted persons" to "trust violators."

The fraud triangle's opportunity element may be easier for internal auditors to identify, as it often arises through a lack of controls. It may be more difficult to discern when someone is feeling pressured—especially because, in some organizations, working under pressure represents the norm.

predisposition to distrust, but the appropriate use of questioning to see beyond the superficial.

Fraud in Every Audit Internal auditors must begin every audit aware that fraud may exist. They cannot assume that a particular area or individual is incorruptible. Even minor ethics violations can spiral into something much bigger and more damaging to the organization, which is why internal auditors must maintain a thorough understanding of codes of ethics, policies, and procedures; organizational structures and defined roles and responsibilities; and compensation policies.

Internal auditors must remember that they are not only auditing processes, they are auditing people. Even good people can—under certain circumstances—commit unethical and fraudulent acts. Practitioners need to understand that, although most people want to do the right thing, definitions of what is "right" can vary, depending on culture and context. To get to the bottom of potential or actual fraud, internal auditors must have probing conversations with employees, gathering pertinent information but avoiding overreliance on their representations.

TRUST BUT VERIFY

How do internal auditors meet their dual responsibilities of recognizing the red flags of fraud and considering fraud in every audit? They must first open their eyes to the possibility that everyone, in the "right" circumstances, is capable of committing fraud. Then, using this heightened sense of awareness, they can start asking employees appropriate questions and listening carefully to the answers:

- ➔ Do you believe employees of this company behave ethically? If not, do you believe they will be caught? If they are caught, do you believe

Even minor ethics violations can spiral into something much bigger and more damaging to the organization.

with fraud—remembering that no one, even a "good" person, is immune from forces that may lead to misconduct—and considering the possibility of fraud on every audit.

Understanding Behaviors Associated With Fraud Criminologist Donald Cressey's fraud triangle theory indicates that frauds require three elements: pressure, opportunity, and rationalization. Fraudsters are often experiencing some type of pressure, at work or at home, real or imagined. They seek an opportunity to alleviate the pressure (via misdeed), and they must then be able to justify the behavior to themselves ("I deserve it," "Everyone is doing it," "No one will know"). Knowing this chain of events makes it easier to understand how employees who are generally esteemed and respected may suddenly commit

One indicator of pressure may be a sudden change in working hours: arriving early or leaving late may hint at trouble at home or a desire to be alone at the workplace. Or an employee may display a sudden enhancement of lifestyle not commensurate with his or her salary, demonstrated through luxuries such as an expensive car, a high-end watch, an upgraded wardrobe, or an exotic vacation. Fraud may have supplied the original funding for these items, and pressure to maintain them may lead to repeated misconduct. (For additional indicators of potential fraud, see "Red Flags of Unethical Behavior" on page 50.)

How do internal auditors balance their responsibility to identify suspicious employee behavior against their need to maintain good relationships? They apply healthy skepticism, which is not an automatic and cynical

More than **10 percent** of organizations **worldwide** have experienced a significant fraud within the last two years, according to EY's 15th Global Fraud Survey.

IT STARTS WITH CULTURE

Fraud is often enabled, even supported, by the culture of the organization, but understanding that culture is often easier said than done. Part of the problem involves coming to agreement on the definition of *organizational culture*. Most definitions allude to values, attitudes, beliefs, and behaviors—even taboos, symbols, rituals, and myths—that determine how a company's management and staff interact internally and conduct business transactions. Perhaps the most direct definition is that culture is "how we do things around here."

Regardless of the definition, ethics undoubtedly plays a significant part in an organization's culture. Organizational ethics define how the company expects its employees to behave—expectations that are conveyed to employees in written form (policies, procedures, a code of conduct) and behavioral form (tone at the top).

As an ethical concept, tone at the top is frequently cited but not always fully appreciated—even though it is so powerful that its misuse can undermine all the other elements in place to prescribe ethical conduct. Tone illustrates vividly the fact that, when it comes to ethics, what matters most is not what is said, but what is done. One need only glance at Enron's code of ethics, which called for employees to perform in accordance with "all applicable laws and in a moral and honest manner," to see the difference between "walk" and "talk."

Organizations should care about employees' behavior for a multitude of reasons, but a primary concern is that, when unethical behavior goes unaddressed, it can erode the organizational culture—and anything that damages the culture damages the company. In a 2015 Duke University study, *Corporate Culture: Evidence From the Field*, more than 90 percent of CEOs and chief financial officers indicated their conviction that improving organizational culture would improve their companies' value. Why? Because they believe culture influences productivity, creativity, profitability, and growth rates.

Culture is not just a "nice to have"; it ties directly to the bottom line. In a 2017 research report titled, *Transforming Attitudes and Actions: How Senior Leaders Create Successful Workplace Cultures*, 600 senior leaders—from India, Germany, Indonesia, and the U.S.—were asked about their companies' culture and its contribution to success. Ninety-two percent say that organizational culture has a high impact on financial performance, so much so that 84 percent report they are currently taking steps to improve the culture in their organizations.



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



- they will be punished? Why or why not?
- ➔ Do you think transparency exists around the reasons behind key decisions?
- ➔ Do you think compensation is fairly tied to organizational objectives?
- ➔ Are you aware of, or have you noticed, any activity that might indicate that fraud is taking place? Have you noticed any unusual behaviors by other employees, such as a change in lifestyle?
- ➔ Do you think people trust the whistleblower process and have

confidence there will be no retaliation against those who use it? These questions can smooth the path for internal auditors to address tone at the top by enabling them to structure their conversations with senior management around the employees' perceptions of company ethics.

In addition to questioning, various types of tests can be used to identify red flags. Some typical areas to investigate could include:

- ➔ Vendors with the same contact information as employees or multiple vendors with the same contact information.

- ➔ Pre- or post-dated transactions.
- ➔ Consecutively numbered invoices and invoices in amounts just below the threshold for review.
- ➔ Patterns in the data—as identified by data analytics—that may indicate fraud (e.g., invoice amounts that end in .00, transactions made by upper management, transactions made late in the accounting period).
- ➔ Employees' use of their mandatory vacation time.
- ➔ Transactions processed outside normal channels. If such transactions exist, some follow-up questions

RED FLAGS OF UNETHICAL BEHAVIOR

Numerous factors may lead someone to behave unethically in the workplace. Here are just a few, and some associated indicators.

REASONS FOR UNETHICAL BEHAVIOR*	RED FLAGS	POSSIBLE OUTCOME
<p>Unquestioning obedience to authority—Facilitates justifying bad behavior: “I was just doing what I was told.”</p>	<ul style="list-style-type: none"> » The boss supports an environment in which he or she is always right. » Employees parrot the philosophy that “what the boss says, goes.” 	<p>The boss coerces the accountant to make fraudulent journal entries to cover the boss’s theft or to improve organizational performance.</p>
<p>Tunnel vision—A single-minded focus on achieving goals to the exclusion of ethical concerns that may interfere with that achievement.</p>	<ul style="list-style-type: none"> » Employees express feeling excessively pressured to achieve goals. » Human resources has established compensation policies that are tied to completing projects, regardless of their usefulness or profitability. 	<p>The company may set a goal of being the top producer in its industry and encourage doing “whatever it takes” to reach it.</p>
<p>Power of names—The use of nicknames for questionable practices to make them seem more acceptable.</p>	<ul style="list-style-type: none"> » High-pressure, questionable campaigns are given clever, but nondescriptive, names to obfuscate their goals or means of achieving the goal. Generic placeholder names are used for criminal activities. 	<p>Employees become inured to fraud because it is described in terms like <i>greasing the wheels</i> instead of <i>bribery</i> or <i>financial engineering</i> instead of <i>accounting fraud</i>. Other red-flag terms include <i>smoothing earnings</i> and <i>deseasonalizing the data</i>.</p>
<p>Broken window—Physical and social disorder that is taken as a sign that everything is permitted and authority is absent. A single transgression encourages further transgressions.</p>	<ul style="list-style-type: none"> » Employees demonstrate a follow-the-leader mentality that considers “everyone is doing it” as a viable excuse for poor behavior. 	<p>A single fraudulent act spirals into several others, committed by a wider group of people, because the first one was not caught or was not treated as criminal.</p>
<p>The Galatea effect—Employees who see themselves as controlled by their environment or having their choices made for them are more likely to bend the rules.</p>	<ul style="list-style-type: none"> » Executives demonstrate a “victim mentality,” conveying that seeking revenge on anyone (or any organization) perceived to have wronged them is appropriate. » Employees display a low level of engagement in the business. 	<p>Employees commit fraud because they think the company has treated them badly.</p>

*Adapted from Kaptein, M., “Why Good People Sometimes Do Bad Things: 52 Reflections on Ethics at Work,” July 25, 2012.

More than **50 percent** of all **frauds** are perpetrated by people **inside** the organization, according to PwC's 2018 Global Economic Crime and Fraud Survey.

may be useful: How is this transaction normally handled? When is it not done that way? How else could it be done?

Finally, internal auditors can learn quite a bit simply by keeping their eyes open and asking themselves a few questions, such as:


- ➔ Do employees display an unusual degree of deference to leadership?
- ➔ Are values and conduct understood and aligned organizationwide?
- ➔ Does the organization's culture foster a general sense that what is good for the organization trumps everything else—that results are more important than standards?
- ➔ Do management training and leadership programs stress management's responsibility to model and advocate for integrity?

- ➔ Do employees appear to suffer unreasonable pressure to perform? Is management trained to identify and minimize the sources of pressure?

Internal auditors' ability to ask pertinent questions, listen for messages between the lines, watch for both tangible evidence and suggestive behaviors, test objectively and independently, and constantly ask "why?" makes them particularly well-suited to uncovering fraud indicators. Their efforts can go a long way in contributing to the organization's fight against fraud.

RED FLAGS UNFURLED

Ultimately, instituting a program that places fraud recognition and awareness on the front burner does

not require an overhaul in the way internal auditors approach their work. It does, however, require an understanding of the red flags associated with fraud and an acknowledgment that, in every audit, opportunities for fraud, past or present, may exist. And critically, it requires internal auditors to hold on to their inherent trust in people, while recognizing that even those who raise the least suspicion may in fact be quite capable of organizational wrongdoing. 

RICHARD F. CHAMBERS, CIA, QIAL, CGAP, CCSA, CRMA, is president and CEO of The IIA in Lake Mary, Fla.

DEANNA F. SULLIVAN, CIA, CRMA, CPA, CFE, CGMA, is principal at Sullivan-Solutions in Houston.

YOU *Are* INVITED

Join a select group of C-level executives on a three-day immersive experience to prepare for the highest rank of the internal audit profession.

UPCOMING VISION UNIVERSITY SESSIONS:

San Diego
Sept. 10–13
 Loews Coronado Bay
 San Diego, CA

Vancouver
Oct. 29–Nov. 1
 Fairmont Pacific Rim
 Vancouver, Canada

www.theiia.org/VisionU

Where Your Path to CAE Success Begins

VISION UNIVERSITY



**AUDIT EXECUTIVE
 CENTER®**

2018-0337



NAOHIRO MOURI,
the 2018-2019
chairman of The
IIA's Global Board
of Directors, urges
internal auditors
everywhere to
"Emphasize the
Basics – Elevate
the *Standards.*"

Photographs by Gary Spector

Stakeholder pressure on internal auditors has never been greater. In today's dynamic business world, internal audit is called on to ensure businesses around the globe conform to a wide range of legislation and regulation; to provide tactical and strategic insight and foresight into their organization's performance; and to get ahead of the curve on emerging technologies and social trends. And, in fact, the list could go on. ■ Professional internal auditing is based on The IIA's *International Standards for the Professional Practice of Internal Auditing*, which is part of the International Professional Practices Framework. Taken together, these guiding and mandatory principles provide internal auditors the tools to effectively serve their organizations and provide stakeholders confidence that their internal audit

A Standard *of* Performance



team is functioning at the highest possible standards of professionalism and skill. The *Standards* underpin the work that we do every day. Whether auditors are performing a basic audit, provid-

ing assurance, giving advice and insight, or doing a consulting assignment, they need to adhere to certain professional behaviors—just like those followed by doctors, lawyers, accountants, and others.

Professional internal auditors must live and breathe the fundamental values enshrined in the *Standards*. Those values should be crystal clear to everyone in an internal audit function. The theme I've chosen for my term as 2018–2019 chairman of the IIA Global Board of Directors, “Emphasize the Basics—Elevate the *Standards*,” offers a fundamental way of both connecting with our stakeholders and providing the most solid, relevant internal auditing possible.

SETTING AND MEETING EXPECTATIONS

The *Standards* provide consistency in audit practice, guarantee the quality of whatever audit assignment is undertaken, and help the chief audit executive (CAE) align stakeholder expectations with the actual services the audit function provides. Auditors may need to educate stakeholders about what to consistently expect from internal audit and then deliver it—a process the *Standards* greatly enable.

The *Standards* help ground the independent nature of internal audit as it operates as the third line of defense in conjunction with management and the various second line risk and compliance functions. Independence guarantees internal audit's effectiveness. If there is uncertainty about the facts surrounding a particular initiative, for example, or different parts of the business are in dispute, internal audit can be relied on to provide an independent and objective view on the matter at hand. For example, I was recently involved in reviewing an integration project to bring two large organizations into one legal entity. Not only did the board's audit committee ask internal audit to stay very close to the merger, but the regulator asked internal audit to keep it abreast of what was happening by bringing our independent view to the regulator on how the project was progressing. Both sides were concerned that certain controls may be overlooked,

or not be established. Internal audit's position of independence enabled us to provide assurance to both stakeholders and ensure that everyone had the same understanding of what was happening on the ground.

BEING IN CONFORMANCE

Getting the basics right enables internal auditors to tackle emerging issues such as robotics and artificial intelligence from a position of strength. Audit functions that follow the *Standards* will be mature and have excellent connections throughout the business. Without this maturity, the audit function will be unable to respond timely to the rapid technological developments facing organizations.

According to The IIA's rolling research project, the Common Body of Knowledge (CBOK), the percentage of CAEs who say that they are in full conformance with the *Standards* fluctuates. In 2005, 56 percent of CAEs said they were in conformance; this figure dipped to 42 percent in 2010 and then rose to 54 percent in the latest, 2015 survey. However one reads those numbers, they are disappointing, because in any one year only about half of CAEs are achieving what should be the basic professional requirement to operate as an internal auditor.

I am a qualified accountant in the U.S., and I cannot be a member of the American Institute of CPAs without complying with its rules and regulations. The same holds true of other professionals, such as lawyers and doctors. That is why, if we are calling ourselves a profession, my expectation—and that of many stakeholders—is that all internal auditors should be

in conformance with the *Standards*.



OBTAINING EXTERNAL QUALITY ASSURANCE

The CBOK findings seem to indicate that internal audit lead-

ers do not see the value of external quality assurance. In many organizations with small audit functions, stakeholders often are not as demanding, or not knowledgeable, about what internal audit does compared to an audit committee for a listed company where quality assurance reviews of internal audit are expected. However, to be a professional internal auditor, one must be in conformance with all of the *Standards*, including those on quality assurance, and that is much easier to achieve than people think. In the many quality assurance projects I have experienced, I have never seen a spectacular failure.

TO COMMENT on this article, EMAIL the author at naohiro.mouri@theiaa.org

Getting the basics right enables internal auditors to tackle emerging issues such as robotics and artificial intelligence from a position of strength.”

THE CIA CERTIFICATION: THE MARK OF THE PROFESSION

The Certified Internal Auditor (CIA) certification is the global designation all internal audit professionals should achieve. It represents our understanding and application of the *Standards* throughout our work, which helps our stakeholders better recognize the value the profession delivers to organizations. The CIA is the premier, globally recognized certification that enables professional internal auditors to rise above the rest and deliver on stakeholder expectations.

Recently, the CIA exam syllabi and topic areas were revised to bring the exams up to date with the current global practice of internal auditing, to clarify the knowledge and skills CIA candidates must possess, to create greater alignment between the CIA syllabi and The IIA’s *Standards*, and to refocus Part Three content on core skills.

The purpose of the exam is to assess individuals who meet the requisite global competencies in current internal audit practice. There are three parts:

- » Part One – Essentials of Internal Auditing
- » Part Two – Practice of Internal Auditing
- » Part Three – Business Knowledge for Internal Auditing

CIA candidates are expected to:

- » Possess current knowledge of The IIA’s Professional Practices Framework and demonstrate appropriate use.
- » Be able to perform an audit engagement with minimal supervision in conformance with the *Standards*.
- » Be able to apply tools and techniques to evaluate risks and controls.
- » Demonstrate knowledge of organizational governance.
- » Apply knowledge in business acumen, IT, and management needed for internal auditing.

Having the CIA certification conveys to our stakeholders that we mean business – and, importantly, that we have the competencies and skills to deliver on the purpose of internal auditing, to protect and enhance organizational value.

The bottleneck can be the quality assurance process, itself, but it need not be too onerous or expensive. CAEs can attend their local IIA chapters and find a suitable peer with whom to partner so they can reciprocally provide that service. There are plenty of resources that explain how to do this on The IIA’s website (www.theiia.org). My challenge to CAEs is to get an external quality assurance review. I can guarantee they will learn a lot about their function and come away with many tangible benefits. For example, if an audit function finds it has not done enough training, it can use the evidence from the quality assurance review to request funds from the

board. The CAE can require everyone who is pursuing a career in internal auditing to sit for the Certified Internal Auditor (CIA) exam.

Also, a quality assurance review will flush out potential conflicts of interest in terms of independence. And it will



help align the organization’s expectations of internal auditing with internationally recognized best practices, so that stakeholders can feel confident calling on

internal audit for the right issues at the right time.

A UNIQUE PROFESSION

There is another reason my theme is “Emphasize the Basics—Elevate the *Standards*.” Internal auditing as a profession is truly global, and by following the *Standards* we set the benchmark for how the job should be done. Internal audit is practiced in similar ways regardless of industry, geography, size of organization, and whether it is for-profit or nonprofit. This is not the case in the legal or accounting professions, for example, where local laws and practices vary widely.

This is one of the reasons why internal auditing is important to me, personally. I am Japanese, but I’ve worked in the U.S., the Middle East, Asia, and Europe. Wherever I go, I can still practice my profession, speak to internal audit colleagues, and learn from what people are doing in various industries



THE STANDARDS

The IIA's *International Standards for the Professional Practice of Internal Auditing* are principle-focused and provide a framework for performing and promoting internal auditing. The *Standards* are mandatory requirements consisting of:

- » Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels.
- » Interpretations, which clarify terms or concepts within the statements.

Auditors must consider both the statements and their interpretations to understand and correctly apply the *Standards*. The *Standards* use terms that have been given specific meanings as noted in its Glossary.

The International Internal Audit Standards Board released a revision to the *Standards*, which came into effect Jan. 1, 2017. For the full text of the IIA *Standards*, visit www.theiia.org/standards.



VISIT
our Mobile App +
InternalAuditor.
org to watch
the 2018-19
Chairman's
Video.



My goal for every reader of this article, and the profession as a whole, is to put the *Standards* center stage of our efforts.”


and regions. Those conversations have a direct relevance to me because the *Standards* enable us to speak a common language.

My first role was as an accountant, which I did not enjoy because I felt it encouraged me to share too narrow a view of the world. When I retrained as an internal auditor, I was amazed. Internal auditing entailed looking at an organization from end to end. CAEs have to see things through the chief executive officer’s or board member’s lens—without having to actually be in that role. That was—and remains—fascinating to me, and there is no other function in the organization that fulfills that role.

ADVANCING THE PROFESSION

My goal for every reader of this article, and the profession as a whole, is to put the *Standards* center stage of our efforts. My tenure as chair is a relatively short 14 months. I would love to

see conformance with the *Standards* rise from 54 percent where it is today, to 75 percent during my tenure. That may be too ambitious, but I believe it is possible if we all work together.

You do not have to be a CAE to help in that process. If you are a junior auditor planning a career in the profession, take the CIA exam and do at least the recommended amount of training. Attend local IIA chapter events, get to know colleagues in different industries, and develop skills. If you are a CAE and have not yet had an external quality assessment—take the plunge. You will not only be doing yourself and your organization a great service, you will be helping to advance the credibility and effectiveness of the global profession. And that is something worth aiming for. 

NAOHIRO MOURI, CIA, is executive vice president and chief auditor of American International Group (AIG) based in New York.



THE CHAIRMAN OF THE GLOBAL BOARD OF DIRECTORS

NAOHIRO MOURI is executive vice president and chief auditor of American International Group (AIG), a global property-casualty, life and retirement, and general

insurance company based in New York.

In a career spanning more than 20 years, Mouri has held several chief auditor positions. Before joining AIG, he was a statutory execu-

tive officer, senior vice president, and chief auditor for MetLife Alico Insurance K.K. Japan. He also led the audit departments at J.P. Morgan Asia Pacific, Shinsei Bank, Morgan Stanley Japan,

and Deutsche Bank Japan. He began his career at Arthur Andersen in Atlanta and Tokyo.

Committed to supporting internal audit professionals, Mouri also has held numerous board and volunteer leadership positions at The IIA, including international secretary (2007-2008), vice chairman-professional development (2008-2009), vice chairman-professional guidance (2015-2016), vice chairman-professional practices (2016-2017), and senior vice chairman of the

Global Board (2017-2018). He has been IIA-Japan director since 2003.

Mouri served from 2001-2006 as the first elected president of the Asian Confederation of Institutes of Internal Auditors (ACIIA). ACIIA recognized him with its “Outstanding Contribution in the Field of Internal Auditing” honor in 2016.

Mouri advocates for the profession through IIA and other industry forums, and he has lectured at several universities in Japan,

including the Meiji University Graduate Program for Professional Accountancy and Senshu University. Mouri coauthored *Korega Kinyukikan no Naibukansa da (Internal Audit for Financial Institutions)*, which is available in Japanese and Mandarin.

Mouri, a Certified Internal Auditor and Certified Public Accountant, has a bachelor’s degree in accounting from Georgia State University.

Six internal audit leaders share how they climbed the professional ladder.

Jane Seago

Illustrations by Sean Yates

Women *at the* Top

There is a gender gap in internal audit positions that grows wider with each step up the corporate ladder, according to the Internal Audit Foundation's 2015 Global Internal Audit Common Body of Knowledge (CBOK) Practitioner Survey. At the staff level, women hold 44 percent of the positions; at the management level, they represent only 34 percent. When it comes to the top rung – chief audit executives (CAEs) – the gap is wider still, with women holding 31 percent of those positions at publicly held companies.

The CBOK study suggests a couple of factors that may indicate this imbalance is a numbers game. First, there are not as many women in management and executive roles simply because many women leave the workforce for other priorities. Another factor may be timing. Many women who are now eligible for higher positions entered the workforce decades ago, when fewer women worked outside the home – hence, the talent pool is smaller.

But is the causality behind the gender gap that simple? The survey indicates that women possess a significantly lesser amount and depth of formal education, business-specific training, and professional certification than men. And women's parental obligations make it difficult for many of them to accommodate the travel demands and long work hours that accompany advancement in the profession. They often are perceived as less competitive, ambitious, and adept at organizational politics – perceptions that may have more to do with traditional roles than reality.

Collectively, women may feel the deck is stacked against them as they strive to advance to the top of the profession, but some have played their cards right. Here are six women who have beaten the odds.



LIZ DANTIN FRANKLIN
Chief Audit Officer
Fidelity National Financial Inc.
Jacksonville, Fla.

Although Liz Dantin Franklin's résumé reflects just two employers—a public accounting firm where she started as a staff auditor and Fidelity National Financial—she has weathered a sea change in how women are perceived in the workplace. “In 1989, the year I started, only two of the eight hires were women,” she recalls. As time went on, women became a bigger proportion of those hired and firms started focusing on retaining them.

Although now she can laugh at some of her adventures in traveling globally while pregnant, less pleasant are the memories of being expected to set aside her gender to compete in a man's world (see “Achieving a Balance” on page 63). “When I was put up for partner, someone I worked for told me I had better not show up pregnant during the selection process,” she says. It was already too late. She hid her pregnancy as long as possible, but the evidence soon showed. She made it to the last round of cuts but was told she

“Do your best and be confident that you have enough skills to make it work.”

—Liz Dantin Franklin

was being deferred two weeks before the new partners were announced because of reductions in the number of partner admittances that year. “I will never know what the real reason was for being deferred,” she states. “But having a child may have interfered with their plans.”

Franklin's skills positioned her favorably for advancement. She cites communication, technical skills, and flexibility as especially helpful in her move up the ladder. Being able to communicate with people at all levels of the organization and to apply her knowledge of internal audit and internal controls were key, while being flexible showed her “willingness to be available to accommodate client requests, as needed,” she says.

Flexibility was in evidence in the partner track, which necessitated multiple relocations, made possible only by a husband who set aside his career to be a stay-at-home father. But, when a seventh relocation was requested, she took an offer from Fidelity National Financial instead.

Today, Franklin mentors younger employees, urging them to focus on what they do well and to become adaptable. She encourages them to find a champion to show them opportunities and guide their experiences. And she advises not being afraid to take chances. “When I make a decision, I don't look back,” she says. “Do your best and be confident that you have enough skills to make it work.”

BRANDI THOMAS

Vice President, Corporate Audit
Delta Air Lines
Atlanta

“As a black female, I don't always receive the instant respect and credibility that others do,” Brandi Thomas says. “I have shown up at industry events and had someone ask me to bring them another drink.” Thomas is accustomed to being “the only” in the room—the only woman, the only person of color. Perhaps that is why “Get up” is her mantra. “That's what I do,” she explains. “I always get up to fight another day.”

Thomas is convinced that diversity is important in internal audit because of the function's broad charter. “Audit is



“I can see that I was always trying to move on from audit, but audit kept finding me.”

—Brandi Thomas

both art and science,” she says. “Without diversity, it is easy to get caught up in only the science.” She also notes the positive impact of diverse candidates seeing people who look like them successfully navigating leadership positions.

Although Thomas provides that role model for internal auditors, her career nearly took a different turn. She began college in a pre-med program. One physics class later, she knew she was in the wrong field. After graduating with a degree in finance, she went on to hold mostly audit and controllership positions—a background that gave her “an appreciation for the business implications of audit findings and for how to write and speak like a businessperson, not an auditor,” she says.

But business focus is not enough. Thomas considers caring a key factor in her success: caring to deliver the best product she could, to respect those around her, and to help those coming after her. She notes this attitude is a strength many women bring to internal auditing. “I feel a responsibility to my company to make sure we are highlighting the right risks and truth-telling about the status of those risks,” she says. “Even if the ultimate message is not popular, I try to make sure no one is caught off guard.”

Given Thomas’ success, that college physics class was fortuitous. “Looking back on my career, I can see that I was always trying to move on from audit, but audit kept finding me,” she says. “Today, I think it is the coolest job on Earth.”



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



KELLY GAUGER

*Vice President, Audit Services
CenterPoint Energy Inc.
Houston*

Kelly Gauger followed a roundabout path to her current position. Starting in external auditing for a public accounting firm, she transitioned from auditor to client, doing financial reporting and accounting in various manufacturing environments.

In 2001, Gauger joined CenterPoint Energy, managing U.S. Securities and Exchange Commission reporting until she was promoted to director of accounting, overseeing both “normal” and regulatory accounting for the business. “Regulatory accounting and reporting are very unique skills,” she explains. “However, gaining knowledge and experience in this area really enabled me to learn the business and helped position me for my current role.” She considers her transition to the internal audit role in 2012 as “a logical progression.”

While Gauger acknowledges that women are sometimes challenged in the workplace, she considers herself fortunate. She has observed instances of favoritism over the years, but says she has never experienced it personally. “If you stay true to yourself and always

“Learn how to delegate. You can’t set strategic direction when you’re down in the weeds.” – Kelly Gauger

strive to exceed your own expectations, the opportunities and recognition will come,” she says. “I also believe that operational roles and certain industries are more prone to gender inequality in the workplace, compared to roles in the corporate arena.”

Gauger regularly mines her own experience to provide her audit team career guidance such as:

- Never turn down an opportunity that comes along. It may not be an assignment you planned, but it could turn out well.
- Attend roundtables and conferences and learn from CAEs you meet there.
- Establish strong, ongoing relationships with stakeholders such as the audit committee chair, senior management, and key clients.
- Never stop learning. Internal auditing is changing fast. “You can become part of it or become obsolete,” Gauger says. In fact, adaptability is what she looks for in her staff. “What I looked for 10 years ago is completely different from what I need now.”
- To earn promotion, shift from doing to managing. “Learn how to delegate,” she says. “You can’t set strategic direction when you’re down in the weeds.”

Gauger acknowledges that she learns as much from her team members as she teaches them. “I advise building a strong team and empowering them,” she says. “You are only as good as they are.”

Women make up **20%** of C-suite executives, 21% of senior vice presidents, and 33% of senior managers/directors at companies participating in the Lean In/McKinsey & Co. Women in Workplace 2017 study.

MARY-MARGARET HENKE

Senior Vice President,
General Auditor
Western Union
Englewood, Colo.

Mary-Margaret Henke attributes her rise to her current position to the “80-20 rule.” In her experience, 80 percent of the time invested in moving up the career ladder is focused on three things: 1) hard work, which encompasses technical knowledge and soft skills; 2) getting and leveraging a champion; and 3) luck. “I have found that if you have the first two things, you markedly improve your chances of having the third,” she says.

For Henke, hard work began with 10 years at PwC, then continued with

“Do you only want to be right or do you also want to be effective?”

—Mary-Margaret Henke



progressively more responsible roles at CoBank, Janus Capital Group, and Western Union. Along the way, she added skills in preparing and auditing financial statements, implementing U.S. Sarbanes-Oxley Act of 2002 compliance programs, and leveraging IT. When the CAE role opened at Western Union, she had the support of two key individuals and got the job. “I had worked hard for the chief financial officer and controller, so they championed me,” she explains. “Luck came into play when the person previously holding the position left.”

Her success had its challenges. A self-described “tightly wound Type A personality,” at first, she came across to clients, bosses, and co-workers as too aggressive. She does not know if she was judged this way because she is a woman, but she acknowledges that it was true. “I would drive action too quickly because that’s my nature,” she explains. But that does not mean assertiveness is wrong. “You need to be assertive in an intentional way,” she says. “The ‘best of me’ is a person who balances my assertiveness with stopping, listening, and obtaining more information before driving ahead.”

Henke does not regret her mistakes. They have helped her improve what she considers to be one of women’s innate skills—a reliance on nuance rather than brute force. For her, the bottom line is, “Do you only want to be right or do you also want to be effective?”

This viewpoint is especially important in internal audit. Hence her strong support of diversity in the profession. “I need the different perspectives that diversity enables,” she says. Henke will take the insights she gained as a CAE into her new role as Western Union’s senior vice president of corporate applications, governance, and transformational programs.

“High-profile projects give you a chance to show people what you are capable of doing.” —Yulia Gurman



YULIA GURMAN

CAE
Packaging Corporation
of America
Lake Forest, Ill.

As a Russian national and international student, kickstarting a career in the U.S. had additional complexities for Yulia Gurman: English is not her first language and finding a first job necessitated certain legalities. “Some companies do not wish to do visa sponsorships,” she explains, a challenge she overcame by networking. “I became active in campus accounting groups and made contacts

in the accounting firm that ended up hiring me.”

After a few years in the accounting firm, she joined OfficeMax as a senior internal auditor. Not long after she became OfficeMax’s director of internal audit, the company merged with Office Depot and relocated its headquarters. Gurman, with two small children, declined the move and joined Retail Properties of America in a position that enabled her to create the internal audit department from scratch. Three years later, she landed her current position at the Packaging Corporation of America. She notes, “I was looking forward to the next challenge in my career. This was a perfect fit.”

But the new job had its adversity. Frequent changes in leadership within internal audit and the company’s executive team required her to adapt to the new individual’s style and priorities. Filling her team with the necessary talent in a competitive market also proved difficult. “I could overcome that by tapping into a student network we formed by connecting with universities,” she explains. “We promoted the company to them and captured their interest by sharing the great things our team accomplishes.”

Gurman advises women seeking to advance their careers to build a network and seek out mentors. Case in point: The person she replaced in the CAE position was the vice president who hired her for her first internal audit job at OfficeMax. He supported her candidacy for the company’s CAE position.

Gurman also urges women to get involved in high-profile projects, even if they have nothing to do with internal audit. “They give you a chance to show people what you are capable of doing,” she says. In her view, women have the same opportunity as men to become a CAE, but they must take control of their own career, even when it is not easy or pleasant.



JENITHA JOHN

CAE

FirstRand Bank
Sandton, South Africa

Jenitha John credits a good road map for her success in reaching many personal and professional milestones over the past two decades. “I have three mottos that have shaped my journey: persistence pays profits, competence creates confidence, and setbacks sow setups,” she says.

John has needed each of those signposts over the course of her life—starting well before she entered the workplace. “I grew up extremely poor and lost both my parents at a very young age,” she explains. “This meant learning how to fend for myself during my teenage years. It was a catalyst that drove me toward my goals.”

John’s career was built in different industries and economic sectors—Toyota, Eskom, Telkom, Discovery, and now FirstRand—as she held audit and

“Most industries I operate in are still patriarchal. All jobs in the organization are still predominantly male.”

— Jenitha John

accounting positions and served as a nonexecutive director. She also completed a senior executive program at Harvard Business School and earned various professional certifications.

The path to success was not always smooth. John acknowledges the gender disparities. “Most industries I operate in are still patriarchal,” she says. “All jobs in the organization are still predominantly male, including my existing job.”

Despite such challenges, John is convinced women have the emotional intelligence and resilience to overcome all hindrances—to “wake up, dress up, and show up.” And she stresses the importance of diversity in business and internal audit. As organizations transform to respond to changing risks, internal audit must keep pace to reinforce its position as partner and advisor—a goal that John says depends on a diverse mix of skills, experiences, and perspectives.

Her commitment to harnessing diversity goes beyond internal audit, as she spearheads FirstRand’s “Let’s

Women comprise 17% of senior executives at the most admired companies, but only 7% at other companies, according to Weber Shandwick's Gender Forward Pioneer Index 2016.

ACHIEVING A BALANCE

A common theme underscored anecdotally by the women featured in this article and statistically by the CBOK Practitioner Survey is the challenge to balance professional and personal obligations. Women's commitments as spouse and parent make it difficult for them to meet all the expectations, real or perceived, of a rising executive.

Balancing work with being a wife and mother can be heart-breaking, Jenitha John says. "Living with the guilt of basically outsourcing the kids was unbearable," she recalls. "My kids were fortunate to have nannies, tutors, and au pairs to assist at home, but I felt guilty having to have help and juggle a career."

Liz Dantin Franklin agrees, "Of course, family was always a consideration," she says. "Women tended to get married and have children about the time they became senior auditors." But, while daunting, managing work/life balance is not impossible. Franklin points out that she achieved partnership in the accounting firm where she worked while having a family.

The responsibilities of home and family teach valuable lessons, Yulia Gurman says. "I had a boss say to me, 'You're a mom. You know how

"In my experience, working mothers are valued and their need to balance home and work is accommodated, as long as they meet the expectations of the job." —Yulia Gurman



VISIT
InternalAuditor.org to watch video interviews with the women leaders featured in this story.

to deal with kids. I know you will be able to deal with challenges here at the office successfully," she says. "In my experience, working mothers are valued and their need to balance home and work is accommodated, as long as they meet the expectations of the job."

John managed to create an equilibrium that worked for her by "introducing non-negotiables and jealously guarding my time spent with my family." For example, despite having tutors, she signs off on the homework diary before bed and she regularly attends school concerts and sport matches.

As the percentage of women in the profession grows, their rising influence could help balance professional and personal obligations for all internal auditors. As Gurman notes, "Certain responsibilities cannot be delegated. You have to figure out how to make it work. It's all about flexibility, but you need support from the top."

Connect" program. "The program is focused on learning about the differences among people, so we can effectively access and connect with the organization's talent," she explains. "We seek to embed Stephen Covey's philosophy: 'Strength lies in differences, not in similarities.'"

One of John's favorite mementos is a text she received from a staff member because it reminded him of her. "The text included sentiments like: When it's something you truly wish to do, there's a way to get it done. If you don't know how, you can learn. If you don't have time, examine your priorities. If it seems too overwhelming, start with a tiny first step," she recalls. "It made me feel special to know I had influenced someone's aspirations. It's how I've lived my life."

THE REWARD IS OUT THERE

To reach the top of their profession, these six women have expanded their skills, worked long hours in a variety of assignments, navigated the choppy waters of organizational politics, and learned to accept occasional failure as part of the game. They did not do it on their own. Each of them points to how mentors helped them improve their skills, told them hard truths, steered them around pitfalls, and encouraged them to pursue opportunities.

These audit leaders also recognize that some of the qualities generally attributed to women—empathy, communication, and ability to reach compromise and build consensus—have served them well in their careers. And they have hope for women pursuing the profession's top spot: Most see the gender gap narrowing. For women who are climbing the internal audit leadership ladder, the reward is out there, but it must be earned. [la](#)

JANE SEAGO is a business and technical writer in Tulsa, Okla.

Governance Perspectives

BY RICK WRIGHT EDITED BY KAYLA FLANDERS

SELLING ENTERPRISE RISK MANAGEMENT

“Competing with an edge” is the ultimate aspirational value proposition.

Although enterprise risk management (ERM) has a compelling value proposition, it may not always be intuitive to key stakeholders. That often is because the benefits of ERM are not easily observable or clearly quantifiable in the near term. As risk management professionals, internal auditors are easily sold on ERM’s merits because of our role in the third line of defense. We live and breathe risk management governance daily. But internal auditors and other risk professionals engaged in ERM efforts, by nature, do not tend to have strong sales competencies. So, when we propose ways to advance ERM principles to organizational leadership, the message often misses the mark.

The ability to convince stakeholders of ERM’s value may be the difference between an ERM program that flounders as a check-the-box compliance activity and one that develops into a

strategic governance asset. It is vital for internal auditors and other risk management professionals to have a compelling and polished value proposition pitch in their ERM toolbox—one that is intuitive and presentable in terms and language that first and second line of defense managers will embrace.

Risk management is not a new idea, and most business professionals understand its importance. However, some are skeptical, writing ERM off as unnecessary or an academic theory that is unproven in the real world. When this skepticism is not based on an informed position, it is a shortsighted and misguided viewpoint that creates a major cultural barrier when attempting to implement or mature an ERM program. This is when ERM professionals need to be at their best as salespeople.

Just as professional athletes strive for a competitive edge, business professionals also should pursue measures

to enhance their success. ERM can provide the same type of competitive edge that athletes get from personal trainers, data analytics, and other measures. But ERM benefits are realized when organizations appreciate, understand, and embrace the ERM value proposition. For an organization to unlock the potential of ERM as a strategic asset, a key element is a concise value proposition that leaders and managers can easily buy into.

Step 1: Start at the top.

ERM programs are most successful when executive leadership supports them. The ERM value proposition must be understood at the highest management levels. But beyond that, leadership must be compelled to embrace ERM. Only then will leaders develop a vision for pursuing implementation with the requisite energy. Leaders will only embrace ERM when there is a clear value proposition.

READ MORE ON GOVERNANCE Visit InternalAuditor.org/governance



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

ERM'S QUALITATIVE VALUE

ERM makes logical sense from a qualitative standpoint.

Uncertainty (i.e., risk) jeopardizes organizational objectives.

Reduced uncertainty leads to better decision-making.

Better decision-making leads to better risk optimization.

Risk optimization increases the likelihood of achieving organizational objectives.

Achieving organizational objectives leads to strategic success and competitive advantages.

Strategic success and competitive advantages lead to **enhanced organizational value**.

Step 2: Don't oversell. Internal audit must be careful not to sabotage ERM momentum by overpromising what the ERM value proposition can deliver. ERM will not solve all strategic risk management challenges. This message must be communicated with stakeholders by setting realistic expectations about what the organization can achieve. ERM implementation will inevitably encounter failures along with successes.

Step 3: Make the case for ERM by appealing to its intuitive nature. Internal audit should start by making a simple and intuitive case to legitimize ERM. Various entities have given ERM credibility by embracing its virtues. These include regulators (e.g., board requirements for risk oversight), credit rating agencies (e.g., ERM used as rating criteria by S&P and Moody's), and major universities (e.g., ERM academic programs at North Carolina State University and St. John's University). Additionally, ERM's qualitative value is intuitive, as outlined in the waterfall diagram on this page.

Step 4: Draw a distinction between traditional risk management and ERM. All business professionals manage risk. Managers oversee various business functions and manage the risk inherent in these functions. Human resources (HR) managers manage HR risk, finance managers manage finance risk, and so on. The problem with this risk management model is that it does not promote an enterprise view of risk. Risk managers in these siloed functions make risk management decisions that can have negative impacts in other functional areas.

ERM is not designed to replace the traditional risk management model, but rather to enhance it by bringing greater visibility to risk management activities and impacts across functional silos. This is done by implementing risk

management processes to methodically and purposefully identify, respond to, and monitor risks at the enterprise level.

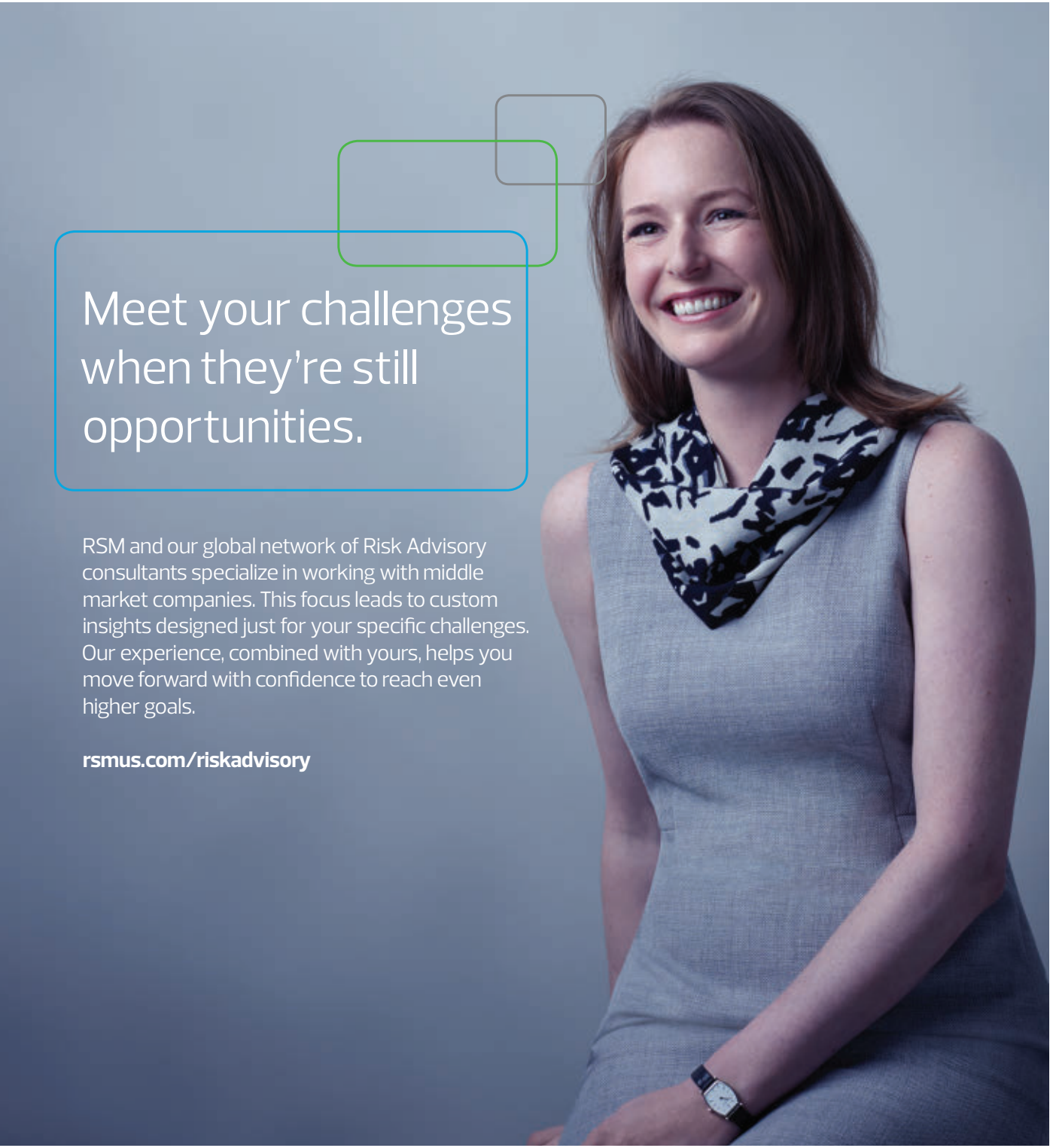
Step 5: Make ERM a tool for aspirational risk management excellence. Compliance benefits may be an acceptable outcome for some organizations, but the real value of ERM is realized when its focus is more strategic. There are three imperatives of a strategic ERM value proposition:

- 1. Make informed decisions.** ERM should support organizational decision-making for strategic planning, tactical execution, budgeting, and risk oversight.
- 2. Protect stakeholder value.** ERM should protect key stakeholders from value erosion.
- 3. Optimize risk outcomes.** ERM should seek the best possible risk outcomes by improving the likelihood of achieving strategic and business objectives, reducing the impact of organizational threats and weaknesses, exploiting organizational strengths and opportunities, and lessening the duration and persistence of negative risk outcomes.

Aspirational and strategically designed ERM programs help organizations compete more aggressively in the marketplace. With the three imperatives in place, an organization is positioned to compete with an edge.

When designed to be a strategic governance asset, ERM facilitates advanced risk-taking capabilities and empowers a thoughtful, safe, and aggressive risk-taking approach. This can result in enhanced competitive agility and ultimately lead to enhanced organizational value. [la](#)

RICK WRIGHT, CIA, is chief audit executive at YRC Worldwide Inc. in Overland Park, Kan.



Meet your challenges
when they're still
opportunities.

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

rsmus.com/riskadvisory

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING





BY J. MICHAEL JACKA

I WAS RIGHT ALL ALONG

Confirmation bias can easily lead auditors to the wrong conclusions.

I used to play a lot of chess. I was never very good. My U.S. Chess Federation ranking hovered around 1200. In other words, not only did Bobby Fischer have little to worry about, neither did my cousin, my friends, and even, on particularly bad days, my dog. But that didn't stop me.

Like the serious chess players, I spent interminable amounts of time with my head bowed over the board pondering each move. It didn't help much. But I continued to do it because protocol dictated that I sit perfectly still ruminating, contemplating, deliberating, cogitating, and in general, looking the part of the keenly focused chess genius.

All these years later, I finally realized one of the roots of my failure. My thinking process was skewed. Rather than exploring alternatives and focusing on the impact of each move, I was spending foot-pounds of mental energy proving to myself that my initial gut feelings were correct. If my first thought was to move my king's knight to Q4, then I would look for every-thing I could to support

that decision—even if I noticed the queen bishop's pawn could indiscriminately destroy said knight.

In psychology and cognitive science, this tendency is known as confirmation bias. And auditors fall into the trap as easily as anyone else. No significant findings will emerge because the data shows the audited department is meeting all its key performance indicators. The prime suspect for committing fraud is the administrative assistant because he is implicated in the initial referral. The audit will reveal significant issues for the department because all previous reviews have included significant issues. We don't need to talk to the client about correcting the identified issues because the solution is obvious.

Looking at these examples, confirmation bias seems obvious. But it can sneak up when we least suspect it. Take, for example, conducting interviews. Many experts say people develop their first impressions about someone within as little as 30 seconds. In fact, one study, conducted in 2006 by psychologists

Janine Willis and Alexander Todorov, found they occur in one-tenth of a second. That's how quickly confirmation bias can take hold, potentially clouding any subsequent facts or evidence that may arise from the interview process.

When we are knee-deep in audit work—when time constraints, budget issues, and the pressures of just getting things done loom over our heads—we take shortcuts. Shortcuts are not necessarily harmful or disadvantageous. Often, gut feel is really just another term for experience. But we have to recognize the shortcuts and take time to ensure our gut reactions are not rooted in confirmation bias.

One of the keys to critical thinking is to take that extra time and to make sure we are thinking about how we think. The last thing we want to do is sacrifice a knight just because it was the first move we saw. [16](#)

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

AUDITORS AND ANALYTICS

Are you taking full advantage of the many opportunities of data analytics?



KEN PETERSEN,
Product Manager,
TeamMate Audit
Solutions, Wolters
Kluwer



DAN ZITTING, Chief
Product Officer, ACL

How can internal auditors identify opportunities for analytics use?

PETERSEN In today's data-driven world, businesses face numerous challenges, from increased regulation and need for transparency to emerging risks from unexpected sources. Auditors should view analytics as an opportunity to reduce risk by aligning test plans with strategic audit goals and auditing larger populations. First, think about your audit objective. Can data help identify where risks exist and how to mitigate them? Second, consider the audit workflow. Look at controls, processes, and procedures for the areas you are auditing to surface ideas for analytics tests to perform. These are generally instituted to mitigate risks, so if they aren't being followed or are being circumvented regularly, the business could be taking on additional risk.

ZITTING Opportunities to use analytics exist throughout the audit plan. A simple

example is anytime you're using the traditional method to pick samples for audit testing, analytics can replace that sample test. Think about data first — not as an afterthought. And when you think in broader terms about providing insight and assurance through data, there's always a data point to be had. For example, if auditing employee talent retention risk, run IT application use metrics to trend employee engagement. If auditing emerging competition threats, use natural language data from Twitter to understand public sentiment. And, if auditing IT system profile vulnerabilities, use correlation analytics to compare IT assets to public vulnerability databases.

How can improper use of analytics damage an internal audit?

ZITTING Whether you work with advanced analytics or old-school spreadsheets, the danger is

the same: drawing conclusions based on bad data. The good news is there's a review and quality assurance process mandated by The IIA's *International Standards for the Professional Practice of Internal Auditing* to prevent us from drawing those bad conclusions. In a digital business environment, those processes need to evolve — making sure we have adequate skills and technical knowledge throughout the team to ensure that effective analytical review and validation steps are taken. If you're overly concerned about analytics damaging your audit, ask yourself if you are instead actually concerned about changing the way you've always done things. Or perhaps you're not sure how to step into this new technology and approach. **PETERSEN** When auditors document their findings they should use very specific language to describe the analytics performed and the

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



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

results vs. any conclusions being drawn from those results. Damage to an audit can occur if conclusions are drawn based on the results of an improper set of tests run against an unreliable set of data. Establishing the scope and determining the validity of the data to be analyzed is critical to the success of the effort. While most analytics tests do not provide proof of any fraud or wrongdoing, analytic results obtained during fieldwork can provide clues about areas that may need further analysis. Also, just because the analytical tests that were performed found nothing of concern, this doesn't always indicate there are no concerns in that area of the business.

How is analytics use changing with innovations such as artificial intelligence (AI)?

PETERSEN AI is in its infancy in the audit world, especially for internal auditors. AI and the various technologies it encompasses (machine learning, deep learning, robotic process automation, natural language processing, image recognition, pattern recognition) will become more ubiquitous over time. AI can become another tool auditors can leverage to enhance their process and improve the time it takes to share results and findings. Future versions of analytics tools will be able to recognize data patterns to identify risks that might not have otherwise been considered or to recognize data that suggests specific tests be performed. Introduction of AI should mean that repetitive work will be performed by machines, allowing auditors to spend more time performing critical analysis and raising the value of the output of audit organizations.

ZITTING AI isn't magic—it's another tool in our toolbox, just like traditional rule-based audit analytics is a tool. AI can be used in countless applications, but finding how it can help gain assurance in areas where we don't always know what to look for is key. Machine learning helps natural language processing (NLP) improve over time. Historically, if I looked at millions of payments to spot which were fraudulent or bribes, I'd have to know what to look for and create a set of rules to run those payments through, flagging violations. I might look for all payments made in high-risk countries where the description includes "donation," resulting in thousands of hits, most of which would not be an issue. But AI and NLP review the same payments and look at everything—the description, vendor, date and time, amount—and tell me which are more likely to be bribes based on criteria I never even considered.

What are the risks of internal audit falling behind with analytics use?

ZITTING The world is moving faster. Historically, you'd go out, do an audit, take six months, and report on it three months later. By the time your audit report is in front of management, it's nine months later. While your findings at

the time may have been totally legitimate, the risk landscape shifted, and the business moved on. The report is now irrelevant. To avoid falling behind, we need to fully embrace and use analytics to move faster and do more. Even if the business doesn't shift its focus between the time you start and finish your audit, there's a good chance you'll report on things the business already knows. Because, while you were out doing your audit, someone ran the numbers and got the answers they needed through analytics. Machines do these jobs much faster than we do.

PETERSEN Today's business environment requires auditors to keep up with the rapid pace of change. In the current data-driven world, organizations are demanding and embracing easier ways to digest and dissect information. Management expects a focus on facts and data-based analysis in all aspects of the business. The traditional practice of simply pulling random samples to support audit testing will soon be considered archaic and of little value. Analytics offers opportunities to identify additional risks throughout the course of an audit, expand the scope of testing, and provide strategic insights. Failing to take advantage of these opportunities will make it challenging to meet increased demands and stay ahead of the changing risk landscape.

How are auditors using analytics to demonstrate their value?

PETERSEN The ultimate objective of internal audit is not to find issues, but to help the business flourish. Traditionally, analytics are performed during fieldwork, and may include testing for duplicate transactions, performing a Benford's test, or looking for other anomalies in the data. However, opportunities exist to consider how analytics can be beneficial in other stages of the audit process such as in scoping, planning, continuous auditing, reporting, or continuous risk assessment. Proactively using analytics to identify areas of focus can help streamline the audit process and apply limited resources to the most important issues. Analytics tools used by audit can be introduced to parts of the business to monitor data throughout the year and head off potential issues before the audit even starts.

ZITTING First, by making audit outcomes quantifiable. Issue ratings of high, medium, and low are almost a thing of the past—they're too subjective. Whereas issues that come out of analytical use have a number or value attached, be it monetary or otherwise. There's a quantifiable nature to our outcomes that makes them more valuable. Next, by getting to insights faster. An audit team that uses analytics is a team with an instantly fast audit robot. By creating automation along the way, auditors can do more work with the same—or fewer—resources. And finally, by providing more assurance over time. Analytics means more coverage. [la](#)

2018 ENVIRONMENTAL, HEALTH & SAFETY EXCHANGE

Connect. Collaborate. Evolve.

.....

OCT. 3–4, 2018

Renaissance Downtown / Washington, D.C.

The Environmental, Health & Safety (EHS) Exchange is the premier conference dedicated to the development and professional practice of environmental, health and safety auditing. The landscape of this industry is shifting and EHS auditors need to be prepared.

Benefits of Attending

- Improved performance in the leadership of EHS practices and EHS auditing.
- Leading practices, data-driven insights, and trends that will position you as a seasoned professional and strengthen your organization's competitive advantage in an increasingly globalized world.
- Expanded EHS peer network and new connections you can turn to for sustainable ideas and strategic insights to serve you for years to come.
- Perspectives from some of the world's leading authorities within and outside of the EHS audit field.

Register today at www.theiia.org/EHSE.



**Environmental
Health & Safety**
AUDIT CENTER

IIA Calendar



IIA CONFERENCES

[www.theiia.org/
conferences](http://www.theiia.org/conferences)

AUG. 13-15 **Governance, Risk & Control Conference**

Omni Hotel
Nashville, TN

SEPT. 14-16 **Internal Auditing Education Partnership Exchange**

Rosen Centre
Orlando, FL

OCT. 1-2 **Financial Services Exchange**

Renaissance Downtown
Washington, DC

OCT. 3 **Women in Internal Audit Leadership Forum**

Renaissance Downtown
Washington, DC

OCT. 3-4 **Environmental, Health & Safety Exchange**

Renaissance Downtown
Washington, DC

OCT. 21
Emerging Leaders
Aria Resort & Casino
Las Vegas

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

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

IIA TRAINING

www.theiia.org/training

AUG. 6-9
Statistical Sampling for Internal Auditors
Online

AUG. 6-31
CIA Learning System Comprehensive Instructor-led Course – Part 3
Online

AUG. 7-10
Various Courses
Chicago

AUG. 13-22
Audit Report Writing
Online

AUG. 14-15
COSO Enterprise Risk Management Certificate Program
Washington, DC

AUG. 21-24
Various Courses
Boston

AUG. 21-30
Enterprise Risk Management: A Driver for Organizational Success
Online

AUG. 28-31
Tools & Techniques I: New Internal Auditor
Portland, OR

SEPT. 4-27
CIA Learning System Comprehensive Instructor-led Course – Part 2
Online

SEPT. 10-13
Vision University
San Diego

SEPT. 10-19
Root Cause Analysis for Internal Auditors
Online

SEPT. 10-26
COSO Internal Control Certificate
Online

SEPT. 11-12
Data Analysis for Internal Auditors
Online

SEPT. 11-14
Various Courses
Dallas

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

SEPT. 18-21
Various Courses
Minneapolis

SEPT. 18-27
Building a Sustainable Quality Program
Online

SEPT. 19-27
Various Courses
Orlando, FL

SEPT. 25-28
Various Courses
New York

SEPT. 26
Fundamentals of Internal Auditing
Online

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



BY STEVEN L. LEIGER

ARE YOU SECURE?

Internal auditors need to prepare themselves for the risk of political pressure.

Nearly every internal auditor will experience political pressure at some point during his or her career. The situation may involve a request to bury audit findings, threats of retribution for perceived disloyalty, or even physical intimidation. In a worst-case scenario, escalation could lead to loss of employment. Nonetheless, practitioners must be willing to meet these challenges, deliver tough messages when necessary—even if it means risking damage to their career—and position themselves to withstand the discomfort and distress. In other words, auditors need to establish a foundation of security, both personal and professional, to weather tough political times.

To be clear, security should not be confused with complacency. The IIA's *International Standards for the Professional Practice of Internal Auditing* sets high expectations for internal auditors, and those expectations should be met by all practitioners. Internal auditors have a duty to both the profession and themselves to perform to their fullest

capabilities and deliver value to stakeholders—both of which are accomplished through hard work and professional competency. Security underpins these efforts, bolstering them with support systems, contingency plans, and a reliable safety net.

Although specific needs will vary, internal auditors can achieve security—both professional and personal—in several ways. Professionally, auditors can increase their peace of mind by obtaining credentials such as the Certified Internal Auditor, familiarizing themselves with the latest best practices, maintaining a network of colleagues for mentorship and camaraderie, and continuously striving to improve. Moreover, practitioners can reinforce their professional development efforts by making sure they enjoy and take pride in what they do and remain grateful for the opportunity to serve the organization.

Personal security is achieved largely through financial planning efforts. The topic has been addressed in many books and research studies and should be a priority for anyone, regardless of profession.

Simply stated, internal auditors, like anyone else, must attain financial security through the practice of life-long, disciplined saving and investing. Basic steps include ensuring access to cash for life's emergencies, minimizing or eliminating debt, saving a percentage of one's income every month, and maintaining savings to cover monthly living expenses over a reasonable time horizon (i.e., a "rainy day" fund).

Internal auditing is not an easy profession—practitioners are expected to perform high-quality, value-added work while maintaining integrity and withstanding adversity. But we are also human, and subject to the influence of political pressure. How might your approach to audit work be different if you had adequate savings, no debt, and a robust professional network? The less political pressure plays a role in audit decision-making, the better the outcome for practitioners, stakeholders, and the organization. [\[a\]](#)

STEVEN L. LEIGER, CIA, CRMA, CFE, is chief audit executive, Nexteer Automotive, in Auburn Hills, Mich.

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



Customize Your Membership with a Specialty Audit Center

.....
INFLUENTIAL. IMPACTFUL. INDISPENSABLE.

The IIA's Specialty Audit Centers provide targeted resources focused on issues that matter most to you and your stakeholders — to keep you influential, impactful, and indispensable.

Learn more at www.theiia.org/SpecialtyCenters



**The Institute of
Internal Auditors**

-
- GOVERNMENT
 - FINANCIAL SERVICES
 - ENVIRONMENTAL, HEALTH & SAFETY

TeamMate+ for Audit

Industry Tested, Auditor Approved



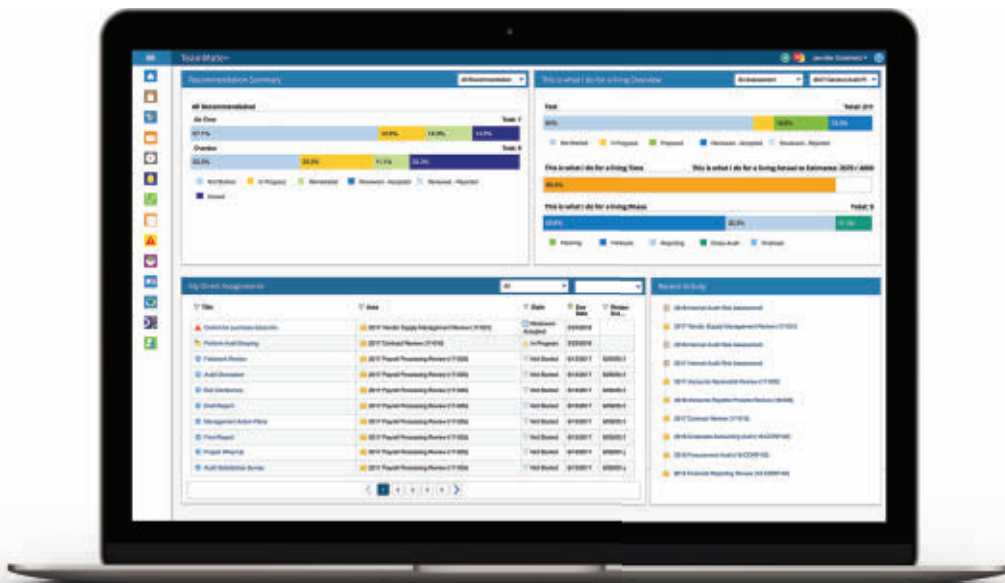
ACCOUNTING TODAY



GOLDEN BRIDGE AWARDS



GRC 20/20



“We like the features in TM+, not only do we like them but we feel they’re necessary for us to advance as a department.”

“TeamMate+ reporting has significantly improved our process allowing us to provide more consistent and thorough analysis to management, auditees, and external auditors. We now have greater visibility across our audit projects.”

Learn more at [TeamMateSolutions.com/Plus](https://www.TeamMateSolutions.com/Plus)