



APRIL 2018

A PUBLICATION OF THE IIA

Cleveland Clinic's Integrity Office

Assessing Risk Appetite and Risk Tolerance

An Audit of the Organization's Analytics

A Five-pronged Approach to Team Development

## INFORMATION DISTILLATION

In audit reporting, it all boils down to what's important to stakeholders.

# SHOUT IT OUT!

May Is International Internal Audit Awareness Month

Spread the word about the value internal auditing brings  
to organizations and the business community.



Download The IIA's 2018  
Building Awareness Toolkit  
now for creative ideas, tips,  
tools, templates, and other  
information for elevating  
and advocating for the  
internal audit profession.

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



## Internal Audit and Cybersecurity

# It's Time to Adapt, Again

Ten years ago, internal audit evolved and adapted to the role IT was playing in business operations. It's time to adapt, again. The Institute of Internal Auditors' (IIA) Audit Executive Center, in collaboration with the Internal Audit Foundation and Crowe Horwath, conducted a limited survey of IIA members to understand how internal audit has begun to adapt to this new cybersecurity risk landscape.

**For a copy of the full report – The Future of Cybersecurity in Internal Audit – visit [crowehorwath.com/InternalAudit-Future](http://crowehorwath.com/InternalAudit-Future).**

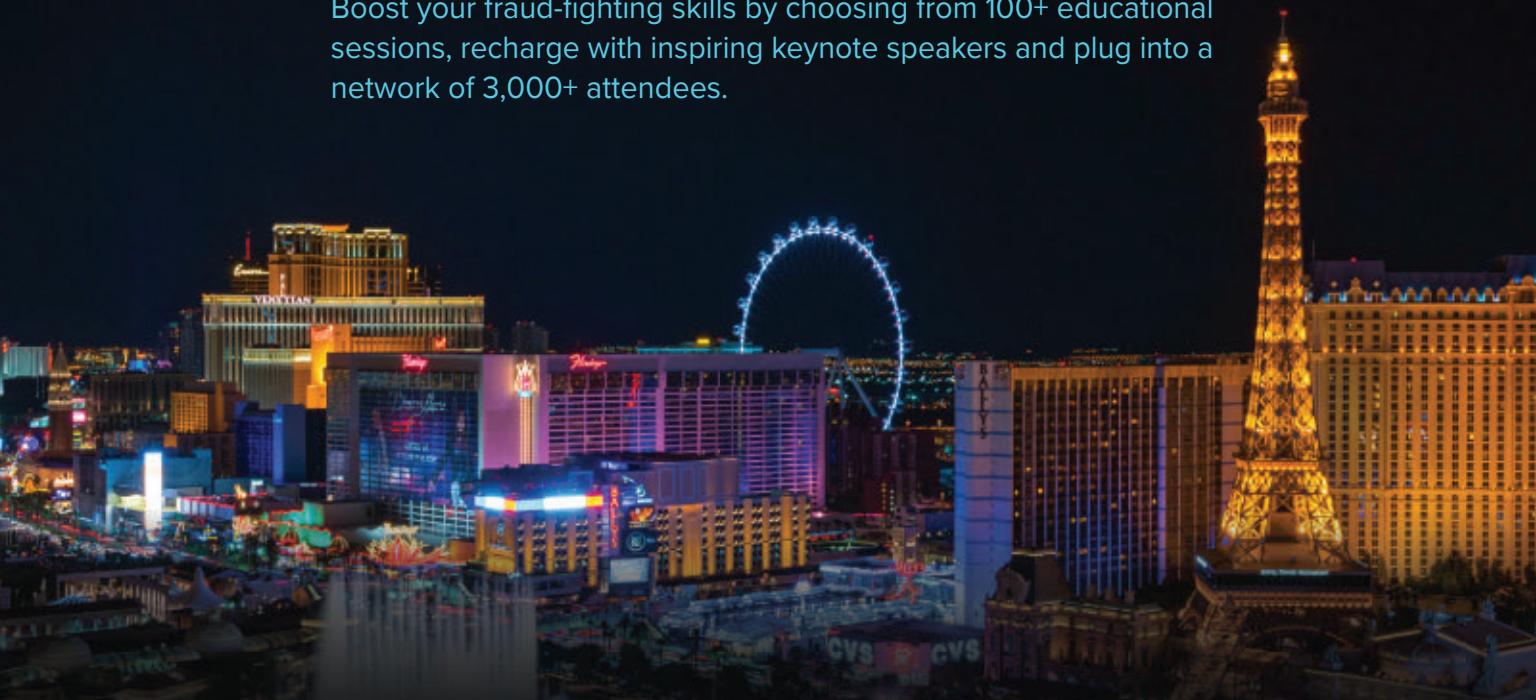
Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

# POWER UP!

YOUR NETWORK • YOUR SKILLS • YOUR CAREER

Power up at the *29th Annual ACFE Global Fraud Conference*. Boost your fraud-fighting skills by choosing from 100+ educational sessions, recharge with inspiring keynote speakers and plug into a network of 3,000+ attendees.



## FEATURED SPEAKERS:



**Rob Wainwright**  
Executive Director,  
Europol



**Clare Rewcastle Brown**  
Investigative Journalist,  
Malaysian 1MDB Corruption Exposé



**Martin Ford**  
Futurist, Artificial Intelligence Expert  
Author of New York Times Bestseller,  
*Rise of the Robots*



**Katherine McLane**  
Crisis Communications and  
Reputation Management Expert  
The Mach 1 Group

## ACFE GLOBAL FRAUD CONFERENCE

JUNE 17-22, 2018 LAS VEGAS, NV

Register by May 11, 2018  
and **SAVE \$100**

**FRAUDCONFERENCE.COM**



## FEATURES

**24 COVER Information Distillation** Today's audit reports need to boil away the unessential to quickly get to what's important to stakeholders. **BY NORMAN MARKS**

**31 The Integrity Office** Cleveland Clinic leverages the work of Internal Audit and Compliance under one umbrella. **BY DONALD A. SINKO**

**36 Risk Consumption** Understanding the difference between risk appetite and risk tolerance can deter organizations from digesting too much risk. **BY SRIDHAR RAMAMOORTI AND RICK STOVER**

**43 Behind the Data** While organizational analytics can yield powerful insights, they may also be a source of risk. **BY JANE SEAGO**

**48 Elevating Team Performance** A European bank CAE shares his five-pronged approach for assessing and developing team members. **BY ARA CHALABYAN**

**55 Social Capital Pays Dividends** Relationship building can enable internal auditors to better help audit clients throughout the organization. **BY JOSHUA K. CIESLEWICZ, BRITTANY ANDERSON, AND LINDSY J.S. CIESLEWICZ**



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



When the ground  
beneath your feet  
is shifting, do you  
stand still or leap  
forward?

Navigate the Transformative Age with  
the better-connected consultants.



## DEPARTMENTS



**7 Editor's Note**

**9 Reader Forum**

**67 Calendar**

### PRACTICES

**11 Update** The IIA releases its 2018 Pulse of Internal Audit; synthetic identity-related fraud on the rise; and new draft guidance applies COSO ERM to sustainability.

**14 Back to Basics** Relationship building can lead to increased trust.

**16 ITAudit** Three key elements can lead to improved technology initiatives.

**18 Risk Watch** Auditors need to assess the risks that put employees' well-being in danger.

**21 Fraud Findings** Seasonal employees coordinate a cash register fraud scheme.

### INSIGHTS

**60 Governance Perspectives** Internal audit needs to assess its own risk appetite.

**63 The Mind of Jacka** Internal audit is more art than science.

**64 Eye on Business** Stakeholder expectations are key to audit reporting.

**68 In My Opinion** Internal audit must innovate and evolve to survive.

## ONLINE [InternalAuditor.org](http://InternalAuditor.org)



### Mapping Assurance

Internal audit practitioners can use assurance maps to provide key insights to boards, senior management, and audit committees.

### Cyber Guidance Overload

Internal auditors need to sort through an array of standards and frameworks to audit cyber risks.

### Kickbacks in the News

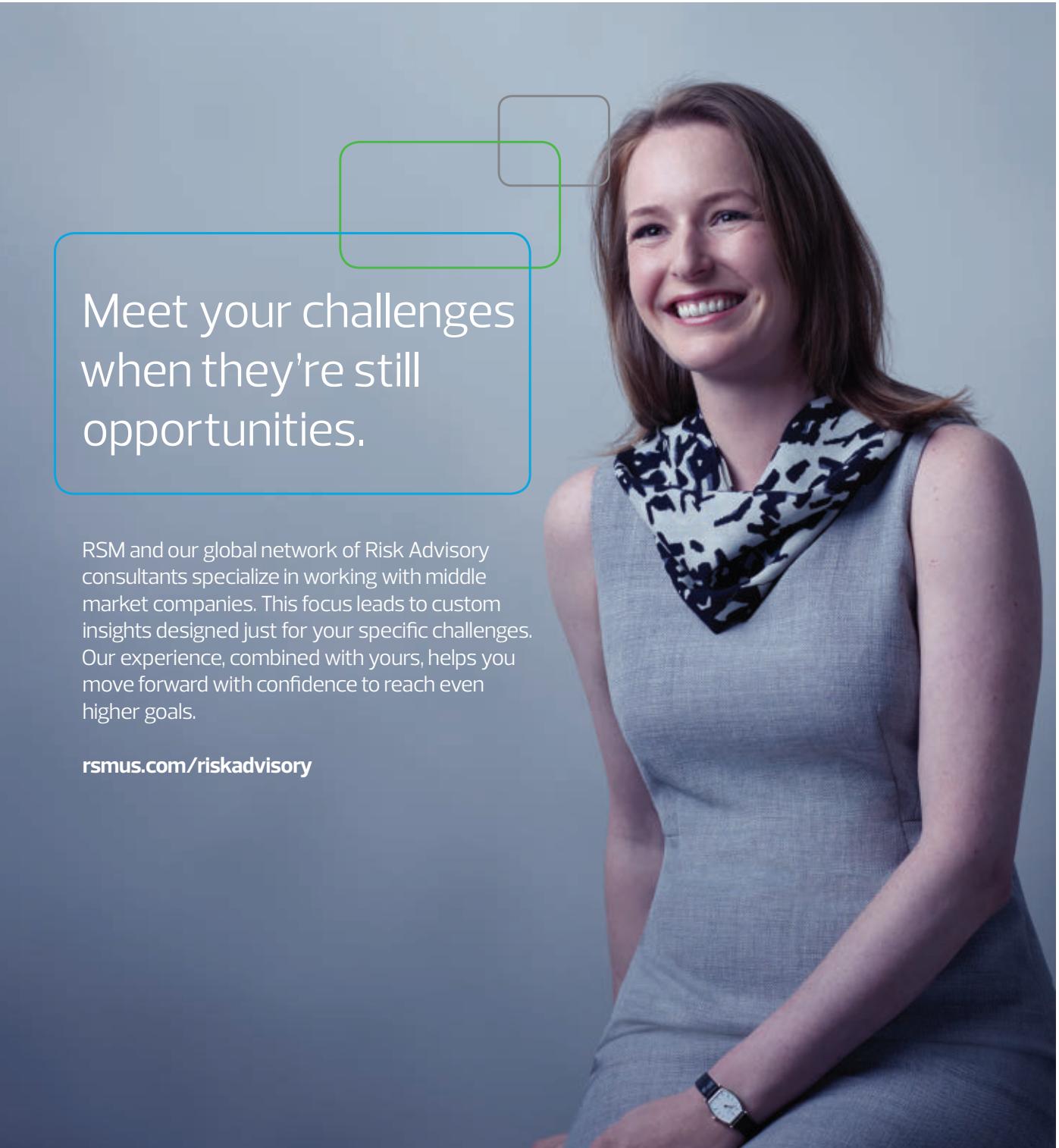
Fraud expert Art Stewart examines a case of media executives accused of taking bribes from a construction contractor.

### Communicating With Stakeholders

Watch an interview with our cover story author, Norman Marks, on providing stakeholders the information they need most.

Find us on Facebook





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](http://rsmus.com/riskadvisory)

**THE POWER OF BEING UNDERSTOOD**  
AUDIT | TAX | CONSULTING



**RSM**



# WORDS MATTER

This month's cover story, "Information Distillation" (page 24), considers the best way to communicate the results of an audit. According to author Norman Marks, effective communication "tells leaders what they need to know, when they need to know it, in a form that is not only readily understood, but also actionable by them."

The editors of this magazine are all about communication. Our job is to provide readers useful information that is easily digestible. Over my 30 years as an editor, I've come to appreciate the importance of using the correct words when communicating. For example:

- » There are certain words writers *utilize* to make them appear smarter, when the simpler form of the word (*use*) works just as well and doesn't appear as pompous.
- » "Very" is not always necessary or correct. Using "very unique," "very critical," or "very first" does not lend to the writer's credibility.
- » Brief is better. Instead of "in order to," use "to" and, instead of "take into account," use "consider."
- » Some words/phrases just don't make sense. It's "regardless," not "irregardless." And, *please*, don't write that you "don't disagree" with something. Either you disagree or you agree.

Whew! I feel better. OK, back to audit communication. In a blog post originally published in October 2011, IIA President and CEO Richard Chambers offered valuable suggestions for what not to include in an audit report that still hold true (see "10 Things Not to Say in an Internal Audit Report," <http://bit.ly/2ozhsyv>). His suggestions include:

- » "Don't use weasel words. It may feel safer to avoid being specific, but when you have too many hedges ... there's a danger that you are not presenting well-supported facts."
- » "The problem is rarely universal. It's good to be specific, but there's a danger in words such as 'everything,' 'nothing,' 'never,' or 'always.'"
- » "Avoid unnecessary technical jargon. Every profession needs a certain amount of technical jargon, but the more we can avoid audit-speak, the more we can be sure that the message is clear."

In this issue's "Eye on Business" (page 64) Michelle Hubble and Sandy Pundmann add their voices to the mix on what constitutes good audit communication. As Pundmann says, "Exclude extraneous words and data that don't add value to the report. ... Crispness is key."

So, what does all of this boil down to? Whether you're an editor or an auditor, words matter. Make sure you choose them wisely.

@AMillage on Twitter



## 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](http://www.theiia.org/SpecialtyCenters)

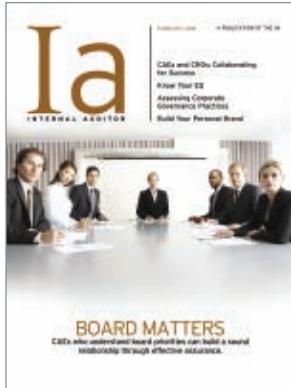


The Institute of  
Internal Auditors

- GOVERNMENT
- FINANCIAL SERVICES
- ENVIRONMENTAL, HEALTH & SAFETY

# Reader Forum

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



## The No Surprises Approach

An interesting article, Mike. EQ may not have been required in the case of Mark and Dave if Mark had discussed the issue with Dave, rather than submitting a draft report and then seeking to meet with him. I apply the no surprises approach and find it works in gaining acceptance and buy-in from my audit clients.

**ANN THIRLAWAY** comments on *Mike Jacka's "How's Your EQ?"* (February 2018).

## Cyber Transparency

I find it interesting that the increased risk is based in part on the increased number of attacks (likelihood) and in part upon the perceived increased impact of the attacks. While risk is

usually considered the product of impact and likelihood, the risk from cyberattacks has been relatively constant over the past few years. What has changed is the openness of the reports of attacks. While these reports are often months (or years) after the hack, that openness is informing management and boards of the risk far better than IT, audit, or risk management can do. The risk hasn't really changed, but companies are understanding it better and taking it more seriously. That helps everyone.

**RICK FOWLER** comments on *Tim McCollum's "The Rising Tide of Cyber Risks"* ([InternalAuditor.org](http://InternalAuditor.org)).

## Earning a Seat at the Table

The best advocates for internal audit are elated (more than satisfied) board and executive team members. When they talk about how internal audit helps them and their organization succeed, we are earning a seat at the table.

**NORMAN MARKS** comments on *the Chambers on the Profession blog post, "Internal Audit Advocacy: Actions Speak Louder Than Words"* ([InternalAuditor.org](http://InternalAuditor.org)).

## Internal Auditors as Freelancers?

A good question would be whether, if an auditor develops entrepreneurial skills, he or she is also going to have the ability to be an entrepreneur. Mike uses good comparison that I had not heard before.

**STEVE SCHOENLY** comments on *the From the Mind of Jacka blog post, "The Internal Auditor as Entrepreneur"* ([InternalAuditor.org](http://InternalAuditor.org)).

## Fake News

I like Richard's last statement, "So, now even the news about the fake news may be fake." Everything seems fake. There is a saying in Amharic, "Tor kefetaw wore yefetaw," which means a defeated people/country in fake news is greater than those defeated in a battle. The question is, how can we redefine our risk appetite in this regard?

**SAMUEL ADEME** comments on *the Chambers on the Profession blog post, "Truth Is, Fake News Has Always Been a Risk"* ([InternalAuditor.org](http://InternalAuditor.org)).



VISIT [InternalAuditor.org](http://InternalAuditor.org)  
for the latest blogs.



INTERNAL  
AUDITOR

APRIL 2018

VOLUME LXXV:II

### 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 Cassells, CIA, CCSA, CRMA, CFE  
Kayla Flanders, CIA, CRMA  
J. Michael Jacka, CIA, CPCU, CFE, CPA  
Steve Mar, CSA, 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, CGA, FCIS, FCMA  
Mark Brinkley, CIA, CCSA, CRMA  
Robin Altia Brown  
Adil Buhariwalla, CIA, CRMA, CFE  
Wade Cassells, CIA, CCSA, CRMA, CFE  
Daniel J. Clemens, CIA  
Michael COX, FIAANZ, AT  
Dominic Daher, JD, LLM  
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, CPCU, CFE, CPA  
Sandra Kasahara, CIA, CPA  
Michael Levy, CIA, CRMA, CISA, CISSP  
Merek Lipson, CIA  
Thomas Luccock, CIA, CPA  
Michael Marinaccio, CIA  
Alyssia G. Martin, CPA  
Dennis McGuffie, CPA  
Stephen Minder, CIA  
Jack Murray, Jr., CBA, CRP  
Hans Nieuwlands, CIA, RA, CCSA, CGAP  
Bryant Richards, CIA, CRMA  
Jeffrey Ridley, CIA, FCIS, FIIA  
Marshall Romney, PhD, CPA, CFE  
James Roth, PhD, CIA, CISA  
Katherine Shamai, CIA, CA, CFE, CRMA  
Debora Shelton, CIA, CRMA  
Laura Soileau, CIA, CRMA  
Jerry Strawser, PhD, CIA, CPA, CRMA  
Glenn Summers, PhD, CIA, CPA, CRMA  
Sonia Thomas, CRMA  
Stephen Tiley, CIA, CISA

### Robert Venczel, CIA, CRMA, CISA

Curtis Verschoor, CIA, CPA, CFE  
David Weiss, CIA  
Scott White, CIA, CFSAs, CRMA  
Rodney Wright, CIA, CPA, CFSAs  
Benito Ybarra, CIA

### IIA PRESIDENT AND CEO

Richard F. Chambers, CIA,  
QIAL, CGAP, CCSA, CRMA

### IIA CHAIRMAN OF THE BOARD

J. Michael Peppers, CIA,  
QIAL, CRMA

  
PUBLISHED BY THE  
INSTITUTE OF INTERNAL  
AUDITORS INC.

## CONTACT INFORMATION

### ADVERTISING

[advertising@theia.org](mailto:advertising@theia.org)  
+1-407-937-1109; fax +1-407-937-1101

### SUBSCRIPTIONS, CHANGE OF ADDRESS, MISSING ISSUES

[customerrelations@theia.org](mailto:customerrelations@theia.org)  
+1-407-937-1111; fax +1-407-937-1101

### EDITORIAL

[david Salierno, david.salierno@theia.org](mailto:david.salierno@david.salierno@theia.org)  
+1-407-937-1233; fax +1-407-937-1101

### PERMISSIONS AND REPRINTS

[editor@theia.org](mailto:editor@theia.org)  
+1-407-937-1232; fax +1-407-937-1101

### WRITER'S GUIDELINES

[InternalAuditor.org](http://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.

# ON THE RISE

# Who Are Internal Auditing's 2018 Emerging Leaders?

# What defines an **extraordinary** internal auditor?

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

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

Nominate by May 11, 2018, at [www.InternalAuditor.org](http://www.InternalAuditor.org)



Executives' cyber risk disconnect... Banks battle credit application fraud...  
Companies taking social stands... COSO ERM guidance for sustainability.

# Update



## INTERNAL DISRUPTORS

Chief audit executives (CAEs) need to take the lead on business disruption or risk internal audit becoming irrelevant, asserts The IIA Audit Executive Center's 2018 Pulse of Internal Audit report. To do so, audit executives must think differently and become internal disruptors, according to the report released in March at the General Audit Management Conference in Las Vegas.

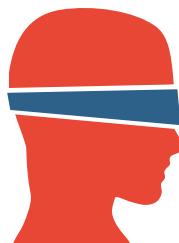
"To be an internal disruptor, CAEs need to break out of their historical frame of reference and be nimble enough to pivot, to refocus, and to reposition internally to create a path toward agile internal

New Pulse report says agility, talent, and innovation are key to internal audit's future relevance.

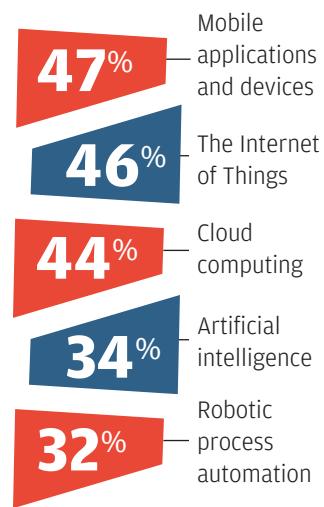
auditing," says IIA President and CEO Richard Chambers.

Making decisive moves about internal audit's agility, talent, and embrace of innovation may be a tall order for CAEs, the report acknowledges. Although two-thirds of the 636 CAEs, audit directors, and senior managers surveyed agree that agility will be very important in the future, only 45 percent describe their internal audit departments as very or extremely agile. But disruption isn't the future—it's here today.

Forty-three percent of CAEs say their internal audit function is fully able to anticipate and react to disruption, while 45 percent



**FLYING BLIND**  
U.S. companies identify emerging technologies for which they are not conducting risk assessments.



Source: KPMG, Tech Risk Management Survey

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



## 33% OF EXECUTIVES GLOBALLY

say their organization has a plan to comply with the European Union's General Data Protection Regulation (GDPR).

## 60% OF EUROPEAN EXECUTIVES

say their organization has a plan in place, but just

## 13% OF EXECUTIVES IN THE AMERICAS

say they have a plan.

"The pace of regulatory change continues to accelerate and the introduction of data protection and data privacy laws, such as GDPR, are major compliance challenges for global organizations," says Reuben Khoo, EY Association of Southeast Asian Nations Fraud Investigation & Dispute Services Leader.

Source: EY, Global Forensic Data Analytics Survey

say they have a strategy for flexible planning and resource allocation necessary to address changing risks. These findings suggest internal audit lacks the fluidity to focus on future risks and opportunities. "Disruptive events do not always provide much advance notice," the report points out.

Key to transformation is developing a more diverse internal audit talent pool. The problem is CAEs still favor candidates with accounting and finance degrees over other

backgrounds, and just 36 percent have a flexible talent management strategy to respond to disruption.

While talent can help CAEs re-envision internal audit's capabilities, they also need to become more innovative. The report advises CAEs to embrace technological advances, assess how the audit function accomplishes its objectives, and continually develop a case for pursuing innovation.

- T. MCCOLLUM

## CYBER MISALIGNMENT

A disconnect exists between cyber risk awareness and management's approach to it.

**T**wo-thirds of senior executive respondents rank cybersecurity among their highest risk management priorities, but just 19 percent are highly confident in their organization's ability to manage and respond to a cyber event, according to a global survey from insurance brokerage and risk management company Marsh and Redmond, Wash.-based Microsoft Corp.

"It's time for organizations to adopt a more comprehensive approach to cyber resilience, which engages the full executive team and spans risk prevention, response, mitigation, and transfer," says John Drzik,



president of Global Risk and Digital at New York-based Marsh.

Findings of By the Numbers: Global Cyber Risk Perception point to a misalignment between cyber risk awareness and management's approach. Seventy percent say IT departments are a primary owner and decision-maker for cyber risk management, compared to the C-suite (37 percent) and risk management (32 percent). - S. STEFFEE

## THE RISE OF SYNTHETIC IDENTITIES

**M**ore than half of banks in the Asia-Pacific region indicate they are experiencing application fraud committed by criminals using synthetic identities, according to a recent poll by credit-scoring

firm FICO. Moreover, one in five banks in the region say between 5 percent and 10 percent of all credit card



Financial companies report an increase in application fraud.

applications are fraudulent, FICO reports.

Synthetic identity fraud involves the creation of an identity based on a composite of multiple individuals, which can be difficult for banks to detect. Fraudsters use the identity to apply

for accounts—including prepaid credit cards and personal loans—to help build validity for the persona. Not surprisingly, 40 percent of respondents identify application fraud as a key priority for 2018.

"Identity fraud was a growing problem in 2017," FICO Asia-Pacific President Dan McConaghay says. "As prevention technologies have improved to stop activities such as card skimming, criminals are now stealing identities or constructing 'fake people' to get real credit cards."

More than 40 percent of respondents say that, among areas vulnerable to criminal theft, mobile apps and social media platforms are most likely to suffer a breach.

Criminals harvest personal data from these sources and use it to create false IDs.

Half of the participants also report an increase of 25 percent to 50 percent in card testing, where criminals test fraud prevention parameters associated with credit cards to determine what transaction activities cause the card to be blocked instead of approved. One-fourth of respondents say card testing has increased by 50 percent to 100 percent.

Forty percent of banks say lack of budget is a key obstacle to addressing fraudulent activity further. The next highest percentage say their organization's fraud department experiences too many false positives.

**- D. SALIERNO**

## THE COMPANY AS ACTIVIST

Companies are increasingly taking stands on issues reflecting their values, says Daryl Brewster, CEO of the Committee Encouraging Corporate Philanthropy (CECP) – The CEO Force for Good.



### Are companies under more pressure to engage in political, social, and economic issues, and what risks does that pose?

Today's on-demand, real-time world has placed pressure on CEOs to quickly assess major social issues within the long-term interest of the corporation, with relevant input from significant stakeholders and consistency with stated values. Patagonia, Salesforce, AT&T, and Pepsi are among recent companies effectively advocating on major issues. CECP has found that identifying material issues, reflecting on a company's values, and addressing key questions can help it navigate these challenging topics by speaking, acting, and partnering based on what is

in the best interest of the corporation. CEOs must understand, assess, and manage the risks of addressing key social issues. In some instances, saying nothing may create a greater risk than speaking out. Increasingly, CEOs run global businesses with customers, employees, and investors registering their support—or not—in real time. While it is in the best interests of companies to support a safe, inclusive, and well-run society, each company must identify its material issues; evaluate those relative values; and assess if, how, and when to respond.

## APPLYING COSO ERM TO SUSTAINABILITY



Environmental and social risks have rocketed up the rankings of most impactful risks in the World Economic Forum's Global Risk Report 2018. To address these threats, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the

New draft guidance aims to help organizations address environmental, social, and governance risks.

World Business Council for Sustainable Development have issued new draft guidance for public comment through June 30.

The guidance applies COSO's updated *Enterprise Risk Management—Integrating With Strategy and Performance* framework to environmental, social, and governance-related (ESG) risks such as weather events and product safety recalls. It highlights methods that organizations can use to identify and assess the severity of ESG risks and describes ways organizations can respond to threats.

"As ESG-related risks are becoming more widespread, organizations need to ensure they have processes in place for identifying, assessing, and managing these complex, entity-level risks and opportunities," says COSO Chairman Paul Sobel. **- T. MCCOLLUM**

# Back to Basics

BY MAJA MILOSAVLJEVIC

EDITED BY JAMES ROTH + WADE CASSELS

## AUDITING IN AN UNCOOPERATIVE ORGANIZATION

Building strong relationships with clients can lead to increased trust and understanding.

For an internal auditor, an uncooperative organization may be characterized as one in which it is difficult to do his or her job. This may be because of a client's resistance to change, lack of trust in internal audit, viewing the function unfavorably, or not understanding the role of internal audit. Any of these scenarios can cause the client to resist working collaboratively with auditors whose job it is to make positive changes in the organization. Internal auditors are supposed to be trusted advisors, so this can be a challenging situation, especially for new auditors.

Turbulent organizational environments or poor communication and cooperation between internal auditors and clients can exacerbate the problem. But lack of trust and understanding about the role of internal audit can cause the most harm. Trust can take years of effort to build and

it is easy to destroy. Even though internal auditors do their job based on facts, they need to have good relationships with other employees in the organization to ensure long-lasting cooperation. When audit clients understand what internal audit does, they are less likely to respond with statements like, "Your findings are not true," "We don't have time for you," or "We're not implementing your recommendations."

Several suggestions may help internal auditors change the mindset of uncooperative employees while building themselves up as trusted advisors.

### Communicate Directly

Talk to people face to face as often as possible. Emails cannot convey moods, feelings, or body language. Auditors should use every opportunity to have direct contact and communication with clients. That will not only enable auditors to talk

to clients more easily, but also puts them in a position to get additional information and react appropriately in difficult situations.

### Empathize and Understand

Understanding the context of someone's reaction is essential when approaching clients. If auditors show understanding of their clients' situation, or auditors recognize the pressure the client is under, it is much easier to gain the client's trust and get buy-in on audit findings. Listening and responding with empathy can foster better working relationships overall.

### Have a Positive Attitude

While working with clients, a positive approach toward the client might be one of the most important aspects of internal auditors' work. Auditors should avoid presenting their findings for effect, restrain themselves from sensationalism, and try to present positive aspects of

SEND BACK TO BASICS ARTICLE IDEAS to James Roth at [jamesroth@audittrends.com](mailto:jamesroth@audittrends.com)



TO COMMENT on this article,  
EMAIL the author at [maja.milosavljevic@theia.org](mailto:maja.milosavljevic@theia.org)

their work. They should explain to clients how implementing corrective actions on findings will benefit them. Auditors should use every opportunity to give positive feedback to their clients and talk about their clients' collaboration to higher management.

**Show Cooperation** Another critical element of a successful audit is cooperation. A willingness to cooperate makes it easier for internal auditors to establish trust with clients. Auditors should be available to their clients. They should provide them with relevant information on time, organize regular status meetings, send reminders, and be available for meetings at their request.

**Be Professional** Internal auditors must remain professional, objective, and independent at all times to conform with Standard 1100: Independence and Objectivity. Even when auditors are kind and positive, they should not abandon their fact-based conclusions in exchange for good cooperation from their clients (see "Social Capital Pays Dividends" on page 55).

**Escalate, When Necessary** If internal auditors cannot accomplish their job by being cooperative, empathetic, and open to clients, they should choose the option of escalation. This might be the only way some clients will take auditors seriously. Depending on the client's personality, it may be

**Contribute to Efficiency** Internal audit findings and recommendations should not only be used for correcting what is wrong, but also for improving or streamlining the use of available resources. If work efficiency can be improved and resources freed up for other purposes, internal audit should point it out. In turbulent organizations, which typically lack resources, these kinds of findings will be appreciated by clients.

**Get Involved** Auditors should involve themselves in all current projects, actions, campaigns, and any other activity the organization is undertaking. This will not only keep auditors updated, but it will also show they are interested in future developments in the organization. However, junior members of internal audit departments should undertake these kinds of initiatives only with permission of internal audit management.

**Be Creative** Internal auditors play a role in creating and organizing the internal audit engagement, from designing the audit program and procedures to workpapers and audit reports. Although no two audits are alike, auditors should make their work as interesting as possible for themselves and their clients. In this way, auditors' work will be much easier and motivating, and feel like less of a burden. Although these kinds of activities primarily relate to lead auditors, junior auditors also can express their creativity through proposing possible work improvements.

### A Strong Relationship

Building trust is a long process. Auditors may encounter many obstacles, unpleasant people, and bad days, but they share with their audit clients a commitment to the same goal—the success of the organization. Practitioners are in a position to promote the profession so that audit clients better understand internal audit's role in business, which can result in less resistance during audits.

By building trust, clients are more likely to view auditors as the advisors and partners that they are. The better an auditor's relationship with his or her clients, the more open they will be to the auditor's critiques and suggestions for improvements. That can not only make the auditor's job easier, but it also is a win-win situation for the organization. **[a]**

necessary to demonstrate the auditor's role and influence to establish an appropriate long-term relationship.

**Be a Change Catalyst** Internal auditors should not be afraid to propose changes. This is especially true in uncooperative organizations. Typically, the environment in uncooperative organizations is characterized by frequent changes, so employees might be even more open to changes than in other organizations. Every auditor might be faced with situations in which proposed changes are challenged from many sides, but this should not be viewed as an obstacle. Effective internal auditors can convince management to take action on issues identified and implement their proposed recommendations.

**MAJA MILOSAVLJEVIC, CIA, CRMA**, is senior internal auditor at Sberbank Europe AG in Vienna.

BY SAM KHAN EDITED BY STEVE MAR

## WHY IT PROJECTS FAIL

By understanding three key elements, internal audit can help improve the success rate of technology initiatives.

Technology plays a vital role in any organization's strategic initiatives, yet every year countless initiatives fail to deliver value. Take Cover Oregon, a \$305 million health insurance exchange website intended to help people find, and sign up for, health coverage. When it failed in 2014, the state resorted to paper forms and hired hundreds of workers to enroll people manually.

Such failure is not limited to business applications. Today, a new car has more lines of code than Microsoft Office, and project failure can lead to death or, in the case of Volkswagen, fraud. The company's diesel emissions scandal has cost it \$30 billion.

Over the past two decades, about 70 percent of IT projects have failed, according to the Standish Group, a Boston-based firm that researches software development project performance. Some of these projects are canceled and never

used, while others fall short of achieving the original business intent. Despite this high failure rate, some organizations have found ways to deliver more projects on time, on budget, and with better outcomes. The Project Management Institute's (PMI's) 2018 Pulse of the Profession report calls these organizations *champions* because of their 92 percent average success rate. Internal auditors can learn from both the failures and successes of these organizations.

### Governance

Governance is about making good decisions. Many organizations have an IT governance function, which provides a formal structure for aligning IT strategy with business strategy. The *International Standards for the Professional Practice of Internal Auditing* requires internal auditors to make sure IT governance sustains and supports the organization's strategies and

objectives (Standard 2110: Governance). IT governance should address the progress and decision-making of projects. At Volkswagen, governance failed at the highest levels, while there was no single point of authority overseeing its development at Cover Oregon. These findings resonate with PMI research reports that show that an actively engaged executive sponsor is a leading factor in project success.

**Measuring Progress** Projects do not fail overnight, but employees often do not accurately report project status information or speak up when they see problems, a Spring 2014 *MIT Sloan Management Review* article asserts. According to "The Pitfalls of Project Status Reporting," when employees see negative outcomes for others who have delivered bad news, they may fear that executives will "shoot the messenger." Such was the case at Volkswagen. Rather

SEND ITAUDIT ARTICLE IDEAS to Steve Mar at [steve\\_mar2003@msn.com](mailto:steve_mar2003@msn.com)



TO COMMENT on this article,  
EMAIL the author at [sam.khan@theia.org](mailto:sam.khan@theia.org)

than telling management that the engineers could not meet the emission standards, they modified the software to manipulate the results, according to a whistleblower's account.

Successful organizations do not hide problems. They have a culture that encourages people to bring problems into the open where they are solved quickly. Internal auditors should assess the culture around project reporting to ensure it is transparent and honest.

**Decisions** A \$10 million IT project will have approximately 15,000 decisions, the Standish Group estimates. With each bad decision, the odds of success diminish. Yet, the most critical decision is whether to start the project at all. For Cover Oregon, this first decision could have changed the outcome of the project. The organization opted to develop a web application from scratch when an existing solution was available.

Internal auditors should review the criteria organizations use for evaluating, selecting, prioritizing, and funding IT investments. Decision-makers need an accurate picture of the resources needed for each proposed project, but estimating these resources is difficult. People tend to be overly optimistic. This is known as the planning fallacy, which can lead to time overruns, cost overruns, and benefit shortfalls.

Internal auditors should counteract the planning fallacy with a stress test. Research from Bent Flyvbjerg and Alexander Budzier, published in the September 2011 *Harvard Business Review*, found that one in six of the nearly 1,500 IT projects they studied had a 200 percent cost overrun and almost 70 percent had a schedule overrun. Based on this data, they devised a stress test. An organization should proceed with a large IT project only if it can absorb a budget overrun of 400 percent and is comfortable only achieving 25 percent to 50 percent of the projected benefits.

## Complexity

Organizations also should consider ways to reduce the project's complexity. Technology is rarely the cause of project failure. It is the complexity of other factors that lead to failure. When planning any change initiative, the organization needs to consider the impact the project may have on the existing organizational culture, the training resources needed, the effect of new regulations, changes to the business environment, the effort to change business processes, and how the organization will manage vendor relationships.

Often, these factors fall prey to the planning fallacy, which can quickly increase the complexity of a large IT project and reduce the chances of meeting the original business intent. An example is the 2013 U.K. National Health Service System, which overran costs by £11 billion (\$15.3 billion) and was delivered nine years late. The complexity resulting

from using four vendors and numerous specification changes led to failure.

The most effective way to reduce complexity is to limit the size of the project, the Standish Group advises. Based on evaluating more than 50,000 IT projects, the firm's researchers found that a small project, consisting of six team members and completed in six months or less, works best. The firm recommends turning large projects into a series of small ones, which can dramatically increase the chances of success.

Research from the Boston Consulting Group aligns with these findings. The firm has developed an online tool called DICE that internal auditors and organizations can use to assess the readiness of a project based on four elements:

- ⇒ *Duration*, or the interval between the project's major "learning milestones" if it lasts six months or longer.
- ⇒ Performance *integrity* of the project team. This element encompasses both the overall skills and traits of the team, and how the team has been configured.
- ⇒ *Commitment* to change shown by the senior management and the people actually undergoing the change.
- ⇒ Additional local *effort* above normal working requirements that is needed during implementation of those undergoing the change, as opposed to the project team.

## Lessons Learned

Although lessons learned are an important part of the project management life cycle, it often is the most ignored part of a project. Organizations with poor success rates do not have a good process for identifying and applying lessons to new projects. Many organizations have not established a repository for sharing knowledge across the business. As a result, valuable knowledge can be lost or forgotten and projects continue to fail for the same reasons. Internal auditors can review whether the organization has a culture of learning from mistakes and how it shares and applies that knowledge to future projects.

## Improving Success Chances

Despite the high risk of IT project failure, internal auditors can help their organization beat the odds by reviewing the governance, complexity, and lessons learned from projects. Specifically, they should evaluate the risks related to large technology projects and perform health checks during key project milestones defined in the project plan. Moreover, they should benchmark the organization's current project success rate against the PMI Pulse of the Profession. A future of more successful technology initiatives starts with improved controls today. [\[a\]](#)

---

**SAM KHAN, CISA, CRISC**, is senior IT auditor at Oregon State University in Corvallis.

BY TOM O'REILLY EDITED BY CHARLIE WRIGHT

## PROTECTING EMPLOYEES

Internal auditors should evaluate enterprise risks to worker safety and well-being.

**A**sk any CEO what the organization's most important asset is, and he or she will likely answer that it's the business' employees. Employees make the cash register ring, invent new products and services, and help meet the needs of the organization's customers and market.

Yet too often, when chief audit executives (CAEs) are asked what organizational asset they most commonly audit, their answers include inventory, fixed assets, receivables, and petty cash. They are far less likely to audit processes for protecting employees.

CAEs can help their organization create a safer workplace by auditing the processes in place for protecting the organization's employees, contractors, vendors, and other third parties on the job. They can start by better understanding the emotional, physical, and financial risks that put workers' well-being in danger and

developing a plan to evaluate the related business processes.

### Workplace Behavior

Of the many troubling events that came to light in recent years, perhaps the most significant was the glaring inability of many organizations to protect their employees from the inappropriate behaviors of others at work. In terms of personal risks, two behaviors stand out: inappropriate sexual behavior and bullying.

Inappropriate sexual behavior includes leering inappropriately, standing too close to others, and touching others in ways that make them uncomfortable—or worse. Nonphysical bad behaviors include telling sexually explicit jokes, using sexual anecdotes, and sharing pornographic images.

The Workplace Bullying Institute (WBI) defines *workplace bullying* as abusive conduct that either threatens, humiliates, or intimidates co-workers, and

other behaviors, such as verbal abuse or sabotage, that interfere with a co-worker's ability to perform his or her responsibilities. A 2017 WBI study notes that 19 percent of U.S. adults have experienced abuse and 37 percent, including witnesses, have been affected by it.

Internal auditors can help their organization prevent or detect inappropriate workplace behavior. Practitioners who have audited ethics processes should know to evaluate whether the organization has a code of conduct that highlights inappropriate workplace behavior. That code should provide information on how to report that behavior and detail its consequences. In addition to confirming that the CEO and senior management clearly and frequently communicate this message, internal auditors should evaluate whether middle managers are doing the same.

The audit scope also should include evaluating

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



TO COMMENT on this article,  
EMAIL the author at [tom.oreilly@theiia.org](mailto:tom.oreilly@theiia.org)

the channels available for employees to report inappropriate behavior. Auditors should determine whether the organization has a hotline, if employees are aware of it, and whether they can report anonymously or without fear of negative repercussions. Are hotline calls addressed timely, investigated thoroughly, and resolved? Are the CEO and the relevant board committee receiving information on hotline awareness, calls, and related investigations periodically?

### Physical Protection

The impact of high-profile events such as the BP oil spill and shootings at businesses, schools, and universities put organizations on notice about the importance of physical safeguards to protect employees. But it's not just low likelihood but high impact events that can result in workers being hurt, hospitalized, disabled, or even killed.

Organizations sometimes put their employees at risk because of unsafe working conditions. This is especially true for employees who operate heavy equipment and machinery, work in construction zones, or work with or near hazardous materials. Organizations also may fail to protect their

is at risk. They should evaluate the security measures in place to protect top executives and their families from being kidnapped or held for ransom.

### Data Privacy

Loss and theft of employee data, including names, Social Security numbers, email addresses, and banking information, puts employees at serious risk of identity theft and fraud. This data allows criminals to take advantage of unaware employees by creating credit card or loan accounts in their names, or collecting medical payments or Social Security benefits. Hackers use sophisticated cyberattacks to steal employee data in bulk or use phishing tactics to steal it from individuals. Employee data also is at risk from other workers who have access to it and intend to misuse it.

Perhaps the easiest way a CAE can help protect employee data is to carry out a data governance and management project. Internal auditors can document what employee data their organization has, where it is located—such as in paper records or on the network—who has access to it, and the controls in place to prevent or detect unauthorized access.

Evaluating the organization's records management program can add value if employee data is stored in physical documents. Other audits include access-rights reviews of applications and systems that store sensitive

employee data, and cybersecurity audits that evaluate how effectively an organization's network protects employee data and detects cyberattacks.

### A Top Risk

Successful organizations understand it's their workers who make them thrive. Unsafe working conditions will make key employees flee, with lower revenues and margins quick to follow. Organizations with effective processes to protect their employees can experience higher employee morale and increased productivity. They also may be less likely to pay fines for noncompliance with related laws and regulations, better ensure the continuity of operations, and prevent damage to their reputation.

If people are an organization's most important asset, then the risks posed to those people should be among the top risks in the business. Internal auditors who can shed light on these risks and how well-controlled these processes are can gain their CEO's and board's attention and support.

## Unsafe conditions will make employees flee, with lower revenues quick to follow.

employees if they are not prepared for events such as tornadoes, hurricanes, geopolitical unrest, and violent acts by employees or others.

Internal auditors can perform many types of audits to evaluate how these security risks are being managed. Auditing to U.S. Office of Health and Safety Administration standards can help identify safety issues in different working conditions and whether workers are following generally accepted safety standards when working in high-risk areas.

Part of an organization's business continuity program should proactively identify the risks from natural disasters and terrorist incidents. The program also should determine whether employees are aware of, and trained on, the organization's crisis management plans. Internal auditors can leverage the ASIS physical security framework or the International Organization for Standardization's ISO 27001 standard on information security management to evaluate the mechanisms in place to deter or detect potential intruders. Moreover, they can recommend managing or restricting access to areas that may harm employees.

One way CAEs can focus the CEO's attention on employee safety is to remind executives that their own safety

**TOM O'REILLY, CIA**, is director and internal audit practice leader with AuditBoard in Boston.



## Audit Management Software

**No Gimmicks**

**No Metaphors**

**No Ridiculous Claims**

**No Clichés**



**Just Brilliant Software.**

*Find out more at [www.mkinsight.com](http://www.mkinsight.com)*

*Trusted by Companies, Governments and Individuals Worldwide.*

# Fraud Findings

BY BRYANT RICHARDS + BOYD BROWN III

## THE HOLIDAY BONUS

A group of seasonal employees coordinates a cash register scheme that brings them more than \$18,000 each year.

**G**rant Gabriel was hired by a small regional gift store chain to start an internal audit function for the growing company. His first task was to perform a risk assessment. As part of the assessment, Gabriel looked at store-by-store comparative financials. In doing so, he noticed that monthly sales and margins for each store seemed consistent, except in one case. The Springfield store had lower margins and sales growth during the holiday season for the previous three years. Gabriel decided to visit the Springfield store and meet with the manager, Mark Adams.

Adams had been the Springfield store manager for seven years. He was a valued employee who led by example with his work ethic and dependability. Often operating without an assistant manager, Adams was known for handling the store on his own.

Upon arrival, Gabriel asked Adams about the lower seasonal margins and revenues. Adams indicated that it was tough to find good help during the holiday season and new, seasonal people make mistakes. He also noted that margins might be a little lower during the holidays because Springfield has many frugal shoppers and the redemption rate of seasonal coupons is high. Adams boasted, "Our redemption rate has been the highest in the company for the last four years."

Adams then explained, "We have a group of five retired women who work the holiday season for us each year. They are great because they are trained, dependable, can handle the customers, and do not need supervision every second." The women had become friends over the years and referred to this job as their "holiday bonus." So, each year before the holidays,

Adams would call and ask them if they wanted their holiday bonus. He also said he paid them 75 cents more an hour than other seasonal employees because they were so good.

Adams went on to explain that since the women started working for him, their shrinkage in gum and candy always dropped during the holidays. Oddly enough, they even had a small overage this year. He attributed it to the seasonal employees deterring kids from stealing gum and candy. "The ladies are shrewd and probably do a good job of keeping watch."

Gabriel asked Adams if he noticed any unusual transactions in the point-of-sale (POS) system. Adams indicated that he was too busy to dig deep into the reports, but didn't notice any major trends in his monthly scan. He mostly checked for a high number of "no

SEND FRAUD FINDINGS ARTICLE IDEAS to Bryant Richards at [bryant\\_richards@yahoo.com](mailto:bryant_richards@yahoo.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](http://InternalAuditor.org).

**Ia**  
INTERNAL AUDITOR



**TO COMMENT** on this article,  
**EMAIL** the author at [bryant.richards@theiia.org](mailto:bryant.richards@theiia.org)

## LESSONS LEARNED

- » Using detailed analysis within the risk assessment process can help quickly direct internal audit toward fraud risk areas.
- » Data analytics cannot solve all problems by itself. Analytics and fieldwork are a powerful combination. Consistent irregularities can always be explained. Whether the answer is fraud or something else, internal audit should never be satisfied without an explanation.
- » Never underestimate the value of objectivity. Many frauds go undetected because management would never believe a certain person would steal. Being

open to the possibility and following the data to its conclusion is the job of internal audit.

- » Detecting fraud early prevents significant future losses as they often continue over time and grow in scale. In addition, it is often difficult to identify the extent of the fraud. Assuming what has been identified is the minimum amount of the fraud keeps the value of fraud detection in perspective.
- » It is always useful to an organization to detect frauds of any size as it allows management to adapt the internal control environment based on the discovered weaknesses.

rings"—when the cash register is opened but a transaction is not entered—to see if cash was being pocketed instead of deposited in the cash register. He did notice more no rings during the holiday season, but that was likely due to higher volume and the inexperienced seasonal employees.

After his interview with Adams, Gabriel performed his own detailed analysis. He looked at three years of data and found two irregularities worthy of follow-up:

- » No rings occurred, but were consistently two to three times per day with the seasonal help and less than one per day with full-time employees.
- » Store coupon redemption was 5 percent higher, but 20 percent higher on cash transactions and normal for credit card transactions, when compared to other stores.

Gabriel returned to the store to observe and ask questions of the employees. Unfortunately, the holiday season was over and the seasonal employees left, so Gabriel didn't expect to uncover much during his observations and discussions with full-time employees. Luckily, one of the seasonal employees, Michele Webster, accepted a part-time position and was working during Gabriel's observation.

"Is this about the cash register scanning problem?" she asked. Gabriel requested an explanation of what she meant. Webster said she saw Caren, one of the holiday employees, scanning gum one day while she was ringing up Tina, another woman from the group of five, and asked her about it. Caren told her the scanner acts up sometimes and could be reset by scanning something, like gum or candy. She also told Webster she could prevent the scanning problem by pressing the no ring button a few times during her shift.

Remembering the inventory variances in gum and candy, Gabriel began to realize why the holiday bonus

comment was funny. After interviewing Adams, the loss prevention director, and numerous employees, a significant and coordinated fraud effort was uncovered. The group of "holiday bonus" employees was running a series of small and difficult-to-detect fraud schemes.

The women would help each other with holiday shopping by ringing up gum or candy for other higher dollar items. The false sales of gum and candy did not create a flag until there was an inventory overage. Holiday shrinkage, or theft, explained the other items.

To avoid detection, they would hit the no ring button on cash transactions and then pocket the cash, but no more than twice a day. If the customer asked for the receipt, they would apologize and claim it was a system error. The transactions were masked by telling other seasonal employees—who they called "kids"—to hit the no ring button twice a day to prevent scanner problems.

Items were then returned at higher values than paid. Apparently, the women would identify an unsuspecting new employee who did not know how to process a return. One would step in to help the new employee by handling the return for him or her on the register. The item was purchased at a significant discount, sometimes fraudulently, and then returned at full price.

Given how carefully the scams were concealed, it was difficult to quantify the total amount. Based on some estimates, though, it appeared that \$18,000 was stolen each year during the holiday season. ■

---

**BRYANT RICHARDS, CIA, CRMA, CMA**, is an associate professor of accounting and finance at Nichols College in Dudley, Mass. **BOYD BROWN III** is an assistant professor of criminal justice at Nichols College.

## Today's audit reports need to boil away the unessential to quickly get to what's important to stakeholders.

**Norman Marks**

**Illustration by Sean Yates**

# A

company president once told me shortly after I joined the organization that he didn't understand why he was receiving copies of internal audit reports. He didn't understand how they were relevant to his work. He had better uses of his time than reading our reports.

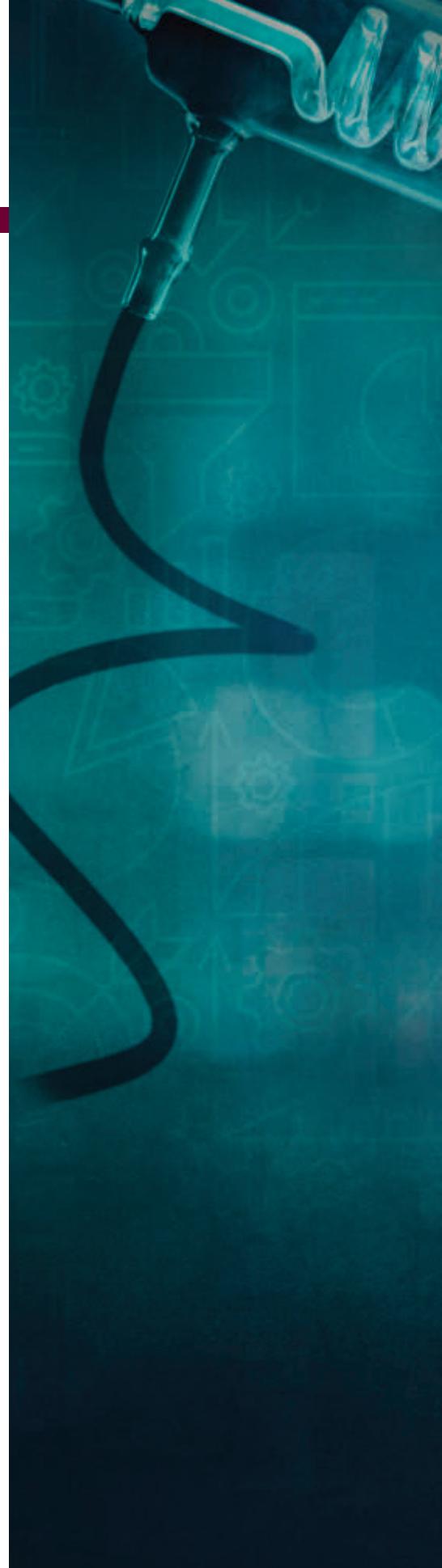
He is not alone. Drew Stein, a board member and former CEO in New Zealand, has written, "Almost all of internal audit findings are mundane operational compliance issues."

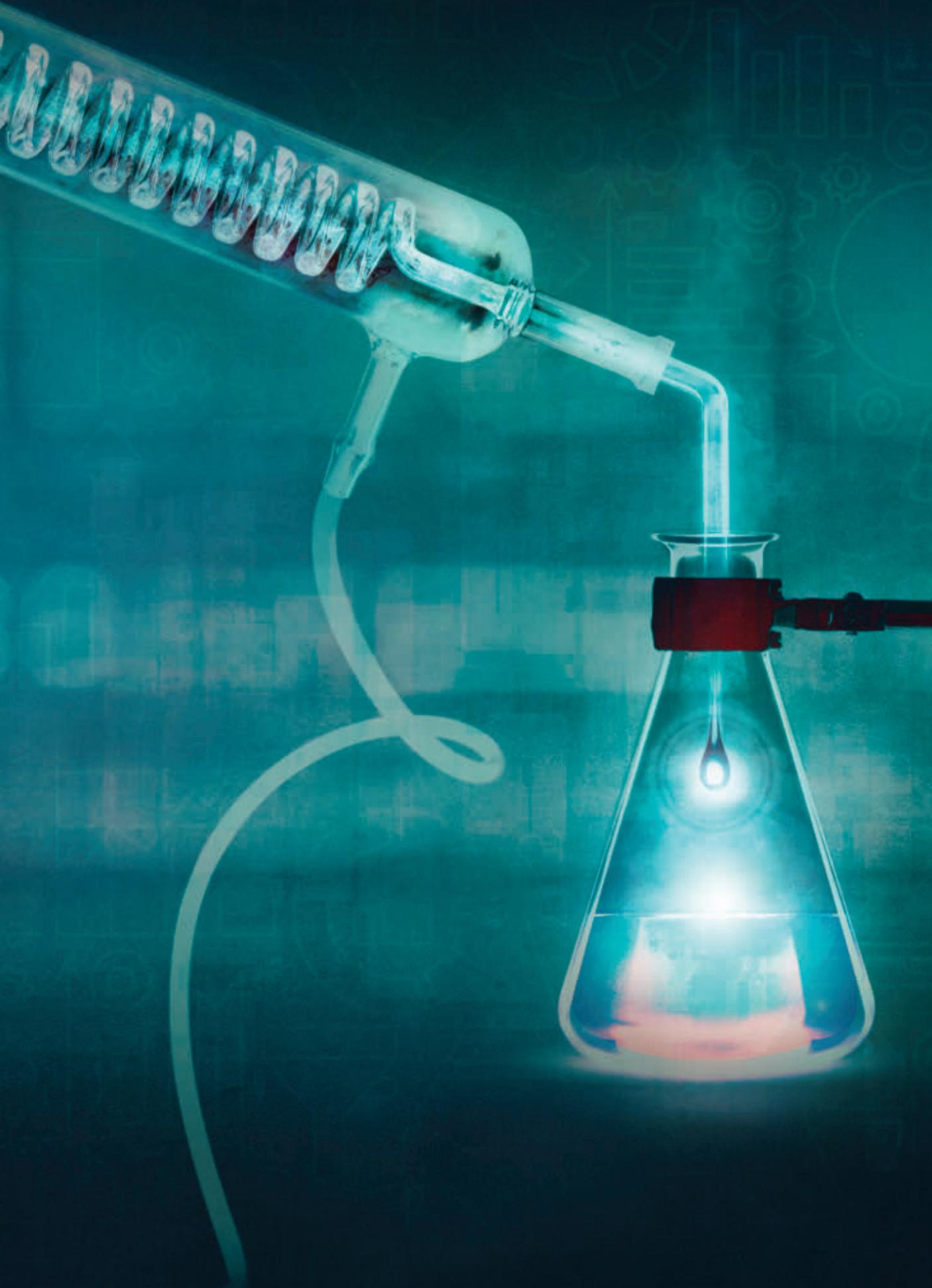
When organizational leaders don't see value *to them* in what internal auditors share—even questioning whether they should waste their time reading audit reports—something is wrong and change is needed. These leaders will only see value if internal auditors' communications are about issues that matter to them and to the organization's success, and provide clear, concise, and actionable information. In other words, auditors must provide them with the information they need to be effective leaders.

In an era of dynamic change, organizations and the managers who run them are also changing how they monitor and run the business. In particular, they must be ready to make decisions quickly because risk and opportunity don't wait for them. A decision delayed is often a decision that is made by a competitor.

In many ways, the internal audit profession has challenged many of its traditional, tried-and-true methods and

# Information Distillation







principles to meet these changing stakeholder demands. One thing that hasn't changed is that many internal auditors are still communicating their findings through a traditional audit report, and that may not be sufficient. They may not realize that the *International Standards for the Professional Practice of Internal Auditing* does not require a formal, written audit report. Standard 2400: Communications requires that "Internal auditors must communicate the results of engagements." The *Standards* require *communication*, and internal auditors should consider how they can *communicate* effectively.

The traditional audit report and its standard format tell stakeholders what *auditors* want to say, rather than telling stakeholders what *they* need to know. A more effective audit communication tells leaders what they need to know, when they need to know it, in a form that is not only readily understandable but actionable by them. In other words, internal auditors should provide stakeholders with the information they need to be effective. At the end of an audit engagement, the auditor should consider what information—assurance, insight, and advice—will help stakeholders lead the organization to success. What are their challenges, and how can internal audit help deal with them?

#### WHAT STAKEHOLDERS NEED TO KNOW

Your young child comes to you crying in the night and tells you she has a tummy ache. Her head seems warm but she doesn't have a high temperature, so you bring her into bed with you and she comfortably cuddles up. But soon she starts crying and curls up into a fetal position. "Mommy, daddy, it really hurts!" she cries. This time when you touch her head, it is hot, and you decide to take her to the emergency room.

Fortunately, she is seen quickly by a doctor, who says he needs to run

a few tests. You wait. Then you wait some more. Eventually, a nurse appears. You run to her and ask, "How is she? Will she be OK?"

The nurse hands you a binder and says, "Here's the doctor's report."

You raise your voice. "Is she OK?"

The nurse smiles and informs you that there is an executive summary on page 3 where you will find the information you need.

The leaders of the organization, internal audit's stakeholders, are not that different. They want to know whether everything—the people, processes, and systems relied on to manage risks—is going to be all right (assurance). They also need to know what they need to do (advice and insight).

They don't need to know:

- » Why internal audit did the audit. They need to know the results and why they matter, not the audit planning process. The results will include assurance on specific risks and objectives.

a glance whether there was anything they needed to worry about. It gave them the assurance they needed to rely with confidence on the controls around derivatives trading risks.

If we identified significant internal control weaknesses, we did more than rely on a rating system. The cover note would have one sentence that described them at a high level. The executive summary would explain how enterprise objectives might be affected.

Going back to the story about the sick child, if you opened the report to the executive summary and it said your child's condition was "needs improvement," would that be acceptable? Would it provide the assurance you need or the information you need to care for her?

#### WHAT DO YOU MEAN?

After I left Tosco, I joined Solelectron Corp., a global electronics manufacturing company. My first task as CAE was to review and approve the audit report for our audit of the Shenzhen, China

## If the executive summary said your child's condition was "needs improvement," would that be acceptable?

- » How internal audit performed the work.
- » Background information that they should already know and is not relevant to the assurance, advice, and insight internal audit is sharing.
- » Details that are being handled appropriately at lower levels of the organization.

The "Cover Note Example" on page 27 accompanied an audit report to stakeholders at Tosco Corp. when I was the company's chief audit executive (CAE). The note showed them at

facility. My predecessor had developed an audit report format that led with the results presented in a table. There was a row for each area of risk that had been included in scope, with an assessment of the related controls—using a red, yellow, green color-coding system—and the number of significant findings.

In the draft audit report I reviewed, the assessment for every area of risk was "red," and the paragraph directly below the table started with, "The system of internal controls at the Shenzhen facility is not adequate. Significant improvements are required."

# Internal audit **communications** “must be accurate, objective, clear, **concise**, constructive, complete, and timely,” according to Standard 2420: Quality of Communications.

## COVER NOTE EXAMPLE

The note below—originally a hard copy, later in an email—was attached to an audit report sent to executive management and the audit committee at Tosco Corp.

January 15, 1995

### Audit of Derivatives Trading

- » Are there any risk issues of significance to the audit committee or executive management? YES/NO
- » Are there any outstanding major internal control findings meriting audit committee or executive management attention? YES/NO

### Distribution:

Audit Committee

I called Audrey, the audit director for Asia Pacific and Japan and a direct report to me. “Audrey, what does this mean?” I asked. Her reply was, after a moment’s hesitation, “Norman, the internal controls are not adequate.” I repeated my question and she repeated her answer.

“Audrey, imagine that as you are getting on the elevator on the fourth floor of the corporate office in Singapore, you see Chester, the president and CEO for Asia Pacific and Japan. He asks you, ‘What do I need to know about your audit of Shenzhen?’ I want you to call me tomorrow and tell me what you would say, recognizing that you only have until the elevator reaches the ground floor.”

Audrey called me the next day. “I would tell Chester that ‘the controls in Shenzhen will not be able to support the 30 percent expansion in manufacturing capacity planned for later this year,’” she said. Instead of blandly saying that controls were inadequate, or even that the listed areas of risk were outside acceptable levels, Audrey was giving executive management actionable information that would help it run the business successfully. This advice and insight was based on an understanding of the organization’s strategies, plans,

and objectives. It told the executive, in clear and readily understandable language, that the plan to move production from other locations to Shenzhen would probably fail. That assessment was then followed with advice on the changes necessary to address the situation. We changed the audit report to lead with the effect on the business and its strategy. We used the language of the business to share our assurance, advice, and insight, rather than the language of internal audit (risk and controls).

The senior management team and the board are focused on executing on and achieving their strategies and objectives. Internal audit may know how internal control and risk management deficiencies may affect those goals, but unless auditors say more than “the system of internal control is not adequate,” there is no assurance that management will appreciate what the audit results should mean to them.

Internal auditors need to communicate the results of their audits in a way that:

- » Makes it clear which enterprise objectives might be affected and how.
- » Explains which risks to objectives are outside desired levels.

- » Helps them identify and then take the necessary and appropriate actions.

For example, our report following an audit of the process for reviewing and approving capital expenditure requests at Tosco led with an opinion statement: “The Authorization for Expenditure process does not meet the needs of the organization. Decisions are not timely and, as a result, business opportunities are lost—rendering null the original business justification.”

The first words used the language of the business to highlight the fact that business objectives likely were not being achieved. The opinion continued by saying that capital decisions might be delayed to the extent that revenue opportunities were lost. The audit report went on to explain what was happening, gave an example of a missed opportunity and the cost to the business, and how management had agreed to address the issue. This report prompted change.

## HAVE A DISCUSSION

Many internal audit departments track and report to their audit committee the number and aging of outstanding audit recommendations. One of the reasons management often fails to take all the necessary actions promptly



is that internal audit and operating management do not have a common understanding of the potential effect on enterprise objectives.

Some auditors talk about internal audit having to “sell” its audit findings. They complain when management is reluctant to make the change they recommend. But perhaps management is right! Maybe the risk is one they should be taking on business grounds, or there is a better way to address the issue.

Rather than writing a recommendation and asking for a management response, internal audit departments

Internal auditors should realize that their final product is not really the audit report and its recommendations—it’s the change that they enable. Informing executive management and the board that internal audit and management have agreed on defined actions is far better than sharing internal audit’s recommendation and management’s response.

### BEYOND THE REPORT

The *Core Principles for the Professional Practice of Internal Auditing* talks about sharing not only assurance and advice,

When there is more to say than “everything is fine,” a face-to-face conversation with management can be the best communication method, especially in private when difficult topics can be discussed candidly. The most effective communications result in a shared understanding, and this is best achieved when both sides not only talk and listen, but ask questions to make sure they understand the other fully. This is the path to effective change and delivering the full value of internal audit to management.

A meeting or a phone call also may be essential if issues are serious and need to be addressed promptly. If the risk is significant, it doesn’t make any business sense to delay corrective action for weeks while the audit report is being drafted.

### FORMS OF COMMUNICATION

Internal auditors need to communicate in a way that is easy for the individual with whom they desire to communicate to receive, absorb, and act on the information they need. Every CAE should take full advantage of modern communication methods as well as embrace the oldest way to communicate—talking and listening.

CAEs should understand how each of their key partners in management and on the board likes to receive information, especially the information they want to get from internal audit. These days, executives receive most of their information in dashboards and similar forms, as well as in meetings and emails. CAEs should consider asking that the CEO’s and chief financial officer’s (CFO’s) daily dashboards or metrics include a section that highlights audit-related issues meriting that executive’s attention. Sometimes, that is enough.

If the executive needs to know that the audit engagement confirmed that controls over a specified risk are

should sit down with operating management and discuss:

- » Do we agree on the facts?
- » Do we agree that there is a risk to one or more enterprise objectives?
- » Do we agree on the significance of the risk?
- » What is the root cause of the problem?
- » Should the risk be accepted or action taken to minimize it?
- » What are the options and which is best?
- » Will the actions bring the risk to an acceptable level?
- » What is a reasonable time frame within which to complete the corrective actions, and who will own each task?

A constructive, open discussion with management—where everybody is listening and working toward the shared objective of enabling enterprise success—is far more likely to result in the change necessary for success.

but insight. Every good internal auditor has opinions that go beyond what is typically included in the formal audit report. These may be of great value to management—if management gets to hear them. For example, the audit team may have thoughts on:

- » The competence of the management team and staff.
- » Teamwork and morale in the area audited.
- » The level of resources available to the team (people, budget, systems, computers, etc.).
- » The ability of the team to deliver optimal performance.

At the same time, management may have questions on these or similar topics and may welcome the opportunity to ask for the audit team’s thoughts. Often, these insights are at least as valuable as the assurance and recommendations for change included in the audit report. But there has to be an opportunity for management to hear and discuss the insights of the audit team.

How auditors communicate results “may vary based on the organizational structure, type of internal audit, and related recommendations,” according to The IIA Practice Guide, Audit Reports.

working effectively, then that can be communicated with a descriptor and a green light. If controls are not adequate and the CEO’s or CFO’s attention is necessary, a red light replaces the green one with a link to the details, which may be the audit report in full or abbreviated form.

#### **LISTEN AND ASK QUESTIONS**

As a CAE, I told my internal audit teams that I don’t ever want them to “go and talk” to somebody. I want them to “go and listen.” If they are talking more than 40 percent of the time, they are talking too much. Internal audit’s communications should provide its audience, its stakeholders, with the opportunity to listen actively—to ask questions and to discuss the situation and its implications.

Communications should start early and be frequent. If internal audit finds something that appears problematic during the audit engagement, it should be talking about it, and listening, to management straight away.

The closing meeting at the end of fieldwork is an excellent opportunity for sharing, not only by the internal audit team but by management. The meeting should conclude with a shared understanding of the facts and issues, the risks they represent to enterprise objectives, and the actions that everyone agrees should be taken. If internal audit has done that well, the audit report simply becomes an after-the-fact summary. Even if there is no formal audit report, everybody should be assured that all issues will be addressed appropriately.

The audit report has value in enabling a discussion with senior management and the board—although serious issues should be communicated promptly in person or by phone. In some industry sectors, the report is necessary to meet the requirements of the regulators. But rather than considering the audit report to be the primary communication vehicle in every case, internal audit should adapt to its stakeholders’ needs for assurance, advice, and insight. When internal audit provides the executive team and the board with the information they need, when they need it, to run the organization successfully, it is optimizing its value. [\[a\]](#)

---

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



**SECURANCE  
CONSULTING**

**OVERCOME YOUR GREATEST RISK.**

**RISK | SECURITY | COMPLIANCE | PEACE OF MIND**

[www.SecuranceConsulting.com](http://www.SecuranceConsulting.com) • 877.578.0215



# The Biggest Risk is Falling Behind

As auditors, we are acutely aware of what happens when audit demand outstrips audit supply. Risk happens.

Faced with increasing expectations, the spotlight is squarely on audit to broaden its focus. That is why we bring you **TeamMate+**, the most intuitive and easy-to-use audit power tool for the profession.

We share your sense of urgency to stay ahead of risk. Using **TeamMate+**, the most advanced platform, empowers you to deliver against strategic expectations.

*"TeamMate+ has significantly improved the productiveness of our department. So much, that our IT Security and Compliance departments are now TeamMate+ customers as well. It has become our GRC application for our organization."*

**- UMC Health System**

*"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."*

**- ORIX USA Corporation**

**TeamMate+**

Learn how you can reduce your risk:  
**TeamMateSolutions.com/Plus**

# The Integrity Office

Cleveland Clinic leverages the work of Internal Audit and Compliance under one umbrella.

**Donald A. Sinko**

While the mission statements of internal audit and corporate compliance functions are similar—focused on operational integrity, efficiency, and effectiveness—organizational structures often put them in separate worlds. In most organizations, the two departments have separate leadership, perform separate risk assessments, develop separate audit and monitoring plans, individually identify and investigate issues and concerns, and recommend appropriate solutions. Rarely does one know what the other is doing. It is unfortunate, because organizations can leverage the work of these two departments, so that working together they can bring value that is greater than the sum of the separate parts.

Twelve years ago, Cleveland Clinic's senior management and the audit committee decided to leverage the work of the offices of Internal Audit and Corporate Compliance by putting them under one umbrella, and calling it the Integrity Office. As the chief audit executive (CAE), I was promoted to a new C-suite position called chief integrity officer to lead the office, and continued to report directly to the audit committee.

## STRUCTURING THE OFFICE

The first organizational decision was whether to combine the two departments into one staff, or keep them as separate departments under one overall leader. Though their mission statements were similar, there was a key difference



in their interpretation and application of the word *independent*. Consistent with the U.S. Federal Sentencing Guidelines, formal guidance issued by the Office of the Inspector General at the U.S. Department of Health and Human Services (DHHS), and requirements imposed in numerous corporate integrity agreements, corporate compliance must maintain an independent reporting structure to the governing body of the organization.

## Just as the missions of internal audit and corporate compliance are similar, so are the skills necessary for their work.

It also must maintain independence and objectivity in all aspects of the organization's compliance and ethics programs. That said, the program cannot effectively be administered or maintained without at least some degree of coordination and collaboration with operational areas. For example, corporate compliance often participates in the development of policies and procedures, internal controls, and systems to mitigate risks. Independence is likewise a necessity for internal audit, but in a different way. The work of internal audit is much more defined than that of corporate compliance and must conform to stringent professional standards of independence. Internal audit must demonstrate independence of mind as well as appearance. Considering that independence and objectivity are core tenets of both professions, we felt it was necessary to preserve a certain degree of independence between them. We accomplished this by organizing them as separate departments within the Integrity Office.

### INDEPENDENCE FROM GENERAL COUNSEL

In many organizations, the compliance function reports to the office of general counsel. Board of director guidance from the DHHS Office of Inspector General has provided that the compliance officer should not be the general counsel, or the subordinate to that position. Corporate compliance independence from the legal department is critical, and the integrity office model provides that independence.

Also, while many companies view the compliance department as a legal function, compliance programs should be focused on implementing regulations in the organization's operations and preventing noncompliance, or aiding early identification of issues. Therefore, having a compliance staff that understands the organization's operations and how the regulations can be implemented is most effective.

### SIMILAR SKILLS

Just as the missions of internal audit and corporate compliance are similar, so are the skills necessary for their work. Internal auditors need to understand an organization's operations to audit its processes effectively. Due to the complexity of an academic medical center's varied operations, Cleveland Clinic's internal audit staff consists of professionals with different backgrounds in finance, billing, coding, nursing, medical research, IT, and forensics. Similarly, the corporate compliance staff includes professionals with experience in nursing, billing, coding, medical research, and law. Both staffs need excellent investigation skills, and the diversity of professional experience provides a depth of knowledge necessary to audit across the risk population effectively and make appropriate recommendations. A major difference is that while both staffs can identify and report issues

Chief **Compliance** officers are more likely than other titles to say they have a formal process for aggregating risk across the company, according to PwC's 2017 Risk in Review report.

and make recommendations, corporate compliance also can be involved in the issue remediation process. Internal audit can subsequently complete a follow-up audit to determine if the recommendations were implemented correctly.

### RISK ASSESSMENT BENEFITS

Cleveland Clinic is a complex, \$8 billion academic medical center, with multistate regional hospitals and international operations. Like many organizations, it has an enterprise risk management (ERM) process that is focused on monitoring significant risks to the organization and what we are doing to address or mitigate those risks. While ERM focuses on the major enterprise risks, internal audit and corporate compliance have to focus on the related sub-risks at ground level.

Internal audit completes an extensive annual risk assessment as the basis of developing its annual audit plan. The risk assessment is a three-pronged process. First, it incorporates input from approximately 100 interviews each year from people throughout the enterprise. In addition to interviews of senior management and board members, we include mid-level managers, administrators, doctors, and nurses. Internal audit learns a lot about the risks they perceive, which can differ depending on their operation. This information is critical to our risk assessment, and we probably would not be aware of many of these perceived risks if we did not listen to such a broad group of people.

Second, we evaluate if we may be affected by national health-care issues or concerns currently impacting other organizations. We frequently read or hear about significant issues at peer organizations, and we want to determine if we may have the same exposures. Evaluating the issues during this process helps mitigate the exposure by either determining that it is not an

issue for us, or that we have identified it and will resolve it more timely.

The third part of our risk assessment process is evaluating known risks from prior years. Have they adequately been resolved? Is a follow-up audit warranted? All three parts of the risk assessment process are important to capture and understand the risk population.

One element of an effective compliance program is to include the auditing and monitoring of compliance risks. Corporate compliance functions also have to perform a risk assessment to determine the risks to be included in their audit and monitoring programs. Risk assessments are much more effective when internal audit and compliance staff can work together to determine the risk population, evaluate

Health Information Portability and Accountability Act (HIPAA). HIPAA security regulations require an organization to have a current assessment of information security risks. At Cleveland Clinic, the chief information security officer reports functionally to the chief information officer, but also has an indirect, or dotted line, reporting to the chief integrity officer. This reporting line provides the chief integrity officer the ability to effectively monitor information security control activities, and the opportunity for internal audit and corporate compliance to make recommendations related to information security-related risks.

### REALIZING SYNERGIES

While our formal risk assessment process happens annually, the benefits of

## It is more effective to have the minds of both departments involved in evaluating risks.

the level of risk, and decide the risks to be audited and monitored. It is more effective to have the minds of both departments involved in evaluating risks. It is also more efficient, as it can eliminate the duplicate steps of both departments auditing the same areas or processes, as well as eliminate certain risks from falling through the cracks and not being audited at all. Management also appreciates when employees are interviewed once during the assessment process instead of internal audit interviewing employees the week after corporate compliance asked them the same questions.

A significant part of any U.S.-based health-care organization's compliance program is complying with the U.S.

internal audit and corporate compliance being under the same umbrella are reaped throughout the year. The findings from one of the department's activities may result in a change in plans for the other department. While internal audit and corporate compliance are separate departments, their offices are on the same floor and they can easily talk with each other about questions or concerns.

We continue to have separate monthly department staff meetings. Because I am familiar with the activities and results in both departments, my attendance at both staff meetings provides the opportunity for immediate transfer of helpful information during discussions. There also is a better



## ENGAGE AND CONNECT GLOBALLY

Gain a competitive edge with unique IIA advertising and sponsorship opportunities as diverse as the 185,000 plus members in nearly 200 countries we serve.

Contact +1-407-937-1388 or [sales@theiia.org](mailto:sales@theiia.org) for more information.

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



**The Institute of  
Internal Auditors**

# 97% of compliance and ethics functions

in Ethisphere's 2017 World's Most Ethical Companies work with internal audit departments to design audits and receive audit results.

understanding of and appreciation for the work performed by members of the other department.

Our internal audit staff has a forensic audit group that is charged with looking for financial, privacy, and information security-related anomalies. They also use their talents to provide corporate compliance support during complex compliance investigations. Our IT audit staff and operations audit staff provide support to compliance investigations when their talents are required to add value.

That support goes in both directions. Our compliance staff members consist of professionals from many disciplines, so they can provide internal audit with invaluable objective insight into areas being audited. Having everyone under the same organizational umbrella also eliminates resource politics. As the chief integrity officer, I can decide the best use of resources and not have to work through another executive's agenda. This is a significant benefit for both departments.

## ENSURING INDEPENDENCE

The Three Lines of Defense model of internal controls puts corporate compliance in the second line of defense, and internal audit in the third line of defense. The main concern with putting corporate compliance and internal audit under common independent leadership is that internal audit cannot then independently audit the compliance function activities. If internal audit cannot independently audit compliance under one umbrella, then it is an internal audit performance issue rather than an inherent limitation with the structure. In addition to the internal reports we provide management and the audit committee, our external auditors review our compliance activities and results. They attend every audit committee meeting, and the audit committee asks for their opinions about the internal

audit and corporate compliance functions during multiple executive sessions throughout the year. If our compliance function were underperforming compared to our peers, our external auditors would inform the audit committee.

Apart from that, management and the board receive other third-party evidence to determine if internal audit is not being above board with its assessment of compliance activities. For example, as a health-care provider to Medicare Advantage programs, insurance plans that provide supplemental coverage to people with government provided Medicare coverage, our compliance program is subject to annual audits by the Medicare Advantage

corporate compliance function has to demonstrate to the steering committee how the organization is addressing and mitigating these risks.

Management and the board also may request to have an external peer review of the compliance program performed. Similar to the process included in *The IIA's International Standards for the Professional Practice of Internal Auditing*, an external peer review of the compliance program would provide an independent evaluation of compliance program effectiveness.

## UMBRELLA OF BENEFITS

The integrity office model was not a common organizational structure at the

**Compliance staff members can provide internal audit with invaluable, objective insight into areas being audited.**

insurance companies. Numerous insurance companies have completed detailed audits of our compliance program, requiring documentation and audit testing support for compliance program requirements. Each of the external auditors issued audit reports showing no findings or recommendations. These reports are provided to senior management and the audit committee as independent third-party support.

We also have a senior-level enterprise-wide corporate compliance committee, chaired by a physician leader. The committee meets twice a month to review compliance program activities and results. The organization's ERM program also has identified regulatory compliance as an area of risk. Compliance risks and current mitigation activities are under the oversight of our ERM Steering Committee. The

time Cleveland Clinic implemented it 12 years ago. Given the success we have experienced and benefits we have realized from having internal audit and corporate compliance under the leadership of an integrity office umbrella, it is easy to see why an increasing number of health-care entities have subsequently adopted it.

In addition to the internal benefits realized, we are pleased that our integrity office model has been an integral part of Cleveland Clinic being recognized as one of the World's Most Ethical Companies by Ethisphere for eight years. It is a recognition that the organization is proud to have received and maintained. **[a]**

**DONALD SINKO, CPA, CRMA,** is the chief integrity officer for Cleveland Clinic in Ohio.

# Risk Consumption

Sridhar Ramamoorti + Rick Stover

Illustration by Timothy Cook



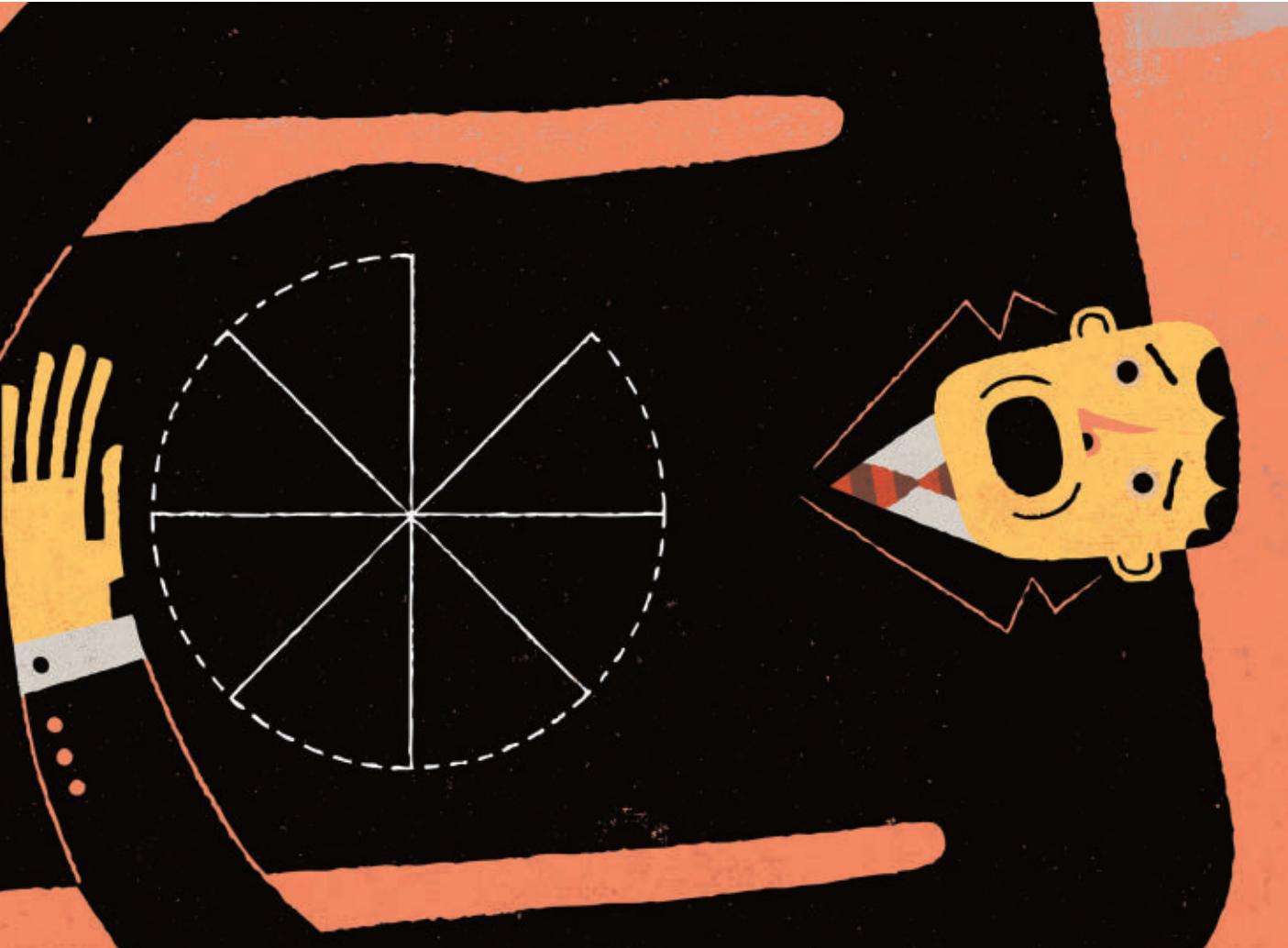
# T

## Understanding the difference between risk appetite and risk tolerance can deter organizations from digesting too much risk.

The concepts of risk appetite and risk tolerance were introduced in 2004 in The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management—Integrated Framework*. Specifically, COSO defines *risk appetite* as "the amount of risk—on a broad level—that an entity is willing to accept in pursuit of value." Naturally, organizations will have different risk appetites depending on their industry, management philosophy, operating

style, culture, and objectives. Therefore, a range of appetites potentially exist for distinct risks, which may change over time. It is conceivable that organizations with separate business segments with various operations or subsidiaries operating in differing industries will have varying levels of risk appetite. In pursuing diverse business objectives, organizations should broadly understand the risk they are willing to undertake.

*Risk tolerance* is the acceptable range of variation in the achievement



of objectives. Both quantitative and qualitative measures are recommended when evaluating risk tolerance. And while risk appetite is about the pursuit of risk, risk tolerance is about what an organization can actually cope with at a more granular level. There is a lot of confusion surrounding risk appetite and risk tolerance, providing an opportunity for internal auditors to educate organizational stakeholders and facilitate risk measurement and management.

#### **AN UPDATED RISK FRAMEWORK**

COSO's 2017 framework update, *Enterprise Risk Management—Integrating With Strategy and Performance*, likely will create a heightened expectation for risk and compliance functions. Internal auditors are expected to educate executive management and the board in this area and to apprise them of key enterprise risk management (ERM) developments. COSO's 2017 ERM revision appropriately reflects the growing realities of the complexities and speed of risks in the global business environment and the need to integrate risk considerations with strategy and performance. Internal audit is positioned to provide an assessment of the propriety of the measures of the organization's risk appetite and tolerance.

The 2008 financial crisis and the subsequent recovery highlight how some of the largest corporations defined and measured their areas of risk and related appetite for risk, but still experienced massive business failures due to their risk management systems crashing. Many of the failures can be attributed to the lack of understanding about the level of risk tolerance an organization can truly accept. Despite setting clear goals, there may not have been any articulation of risk appetite or identification of those responsible when risks were incurred. Since the recovery, organizations have developed even more systems to address and measure their level of risk appetite, but a disconnect

continues to exist as to how much risk tolerance the organization can truly accept—despite the proliferation of chief risk officers in certain industries.

#### **INTERNAL AUDIT'S ROLE**

As the independent function within an organization, internal audit ideally is positioned to assess what level of risk tolerance is truly being accepted by an organization. The unique relationship that internal audit has with operational management, senior management, and the board of directors allows for unbiased reporting of risk appetite and the level of tolerance that can be accepted.

Over the years, organizations were more aligned with documenting and reporting what their risk appetite was and did not extend that to the level of risk tolerance the organization might accept. In other words, organizations became adept at measuring the size of the risk meal, but not the potential

A matrix reporting structure allows for a more robust picture of risk within the organization to senior management and the board. It includes results of internal audit testing presented by functional and business areas (See “Sample Matrix of Risk Reporting Within Organizations” on page 39). A risk issue in purchasing would be reported not solely for purchasing, but also for manufacturing and finance to reflect the wider impact to the organization. Further, this reporting would provide both quantitative and qualitative risk tolerance and risk appetite assessments and indicate whether additional action may be required. To illustrate, an automotive parts manufacturer provides its purchasing department the forecast for its aluminum raw material needs for the next six months. Purchasing is rewarded based on the level of cost controls over major essential purchases and in preventing stock outs of essential purchases. Suppose the purchasing

## **A matrix reporting structure allows for a more robust picture of risk.**

consequences of consuming the whole meal. Taking that analogy further, the result of overconsumption typically leads to indigestion—and it may lead to dire consequences for the organization.

Addressing risk appetite and risk tolerance under the updated COSO ERM framework leads the internal auditor toward a matrix reporting of the organization's risk areas, risk appetite, and risk tolerance. Today, many internal audit functions use reporting tools such as heat maps, which can be adjusted to include qualitative and quantitative measures, enhanced visual presentations, and other forms of output indicating the potential risk tolerance outcomes the organization accepts.

department buys double the amount requested because the supplier offered a special volume discount. On the surface, the organization would have viewed its level of risk appetite in purchasing as low because raw materials are readily consumed. However, the level of risk tolerance being accepted by allowing the purchasing department to overstock has qualitative issues (e.g., rewards based on cost and on preventing stock outs). From a quantitative standpoint, the risk tolerance may be unacceptable given that the over-ordering of aluminum could lead to cash flow problems for payment, logistics costs for storing excessive amounts of inventory, and plant efficiency issues because of the space taken up by excess

Less than **one-third** of organizations globally **maintain** or update risk inventories/registries, according to North Carolina State University ERM Initiative's 2017 Global Risk Oversight Report.

## SAMPLE MATRIX OF RISK REPORTING WITHIN ORGANIZATIONS

RISK ASSESSMENT									
Purchasing Department	Tolerable Risk	Tolerable Risk Variability	Comment/ References	Risk Appetite	Quantitative Measures	Qualitative Considerations	Comment/ References	Cross-function Effect	Comment/ References
Bid Process								Purchasing, Manufacturing, Finance	
Contracting								Purchasing, Manufacturing, Finance	
Quality								Purchasing, Manufacturing, Finance	

inventory. Reporting of this qualitative excess of risk appetite to purchasing, manufacturing, and finance would bring the wider effects into sharp relief. Given the integrated nature of manufacturing operations and incentive compensation systems, such effects must be carefully considered before taking action.

Frequently, the results of internal audit reporting require management to address risk appetite in a cross-functional manner. For instance, an acceptable level of risk appetite in purchasing may be unacceptable in finance. Although the planning phases of ERM typically may involve executive management across functions, this may not be true when results of risk assessments or findings are shared. A concerted effort should be made to share these results broadly to avoid narrow acceptance of findings and unintended consequences. In other words, the same breadth of organizational input that went into planning should exist when evaluating the output and outcomes as well.

### A COMPLEX ASSESSMENT

The basic risk-reward theory from financial economics informs us that

assuming a certain threshold of calculated risk is necessary for business success. Once a certain level of risk within the risk appetite has been assumed, the next step is to worry about how much more risk can be tolerated. Business environments globally are dynamic and ever-changing. As such, both risk appetite and risk tolerance must be evaluated in the context of a shifting landscape, tracking a constantly moving target—a complex assessment that is easier said than done.

Specifically, with regard to risk management policies, reference points, and boundaries, the internal audit function must evaluate existing risk tolerance and risk acceptance relationships to determine whether:

- » Existing risk tolerances are appropriately linked to the organizational risk appetite.
- » Additional risk tolerances need to be created to ensure that the business is effectively managed relative to the risk appetite.
- » The company is operating within the risk tolerance parameters that it has established.

Once it has completed the risk assessment, internal audit then must communicate its findings to help senior management and the board understand the company's current state. Reporting in a matrix format with assessment of risk tolerance and risk appetite by affected functional areas is useful to allow management to address issues in a more holistic manner. For board and audit committee reporting, the need is to be more concise and direct as to where quantitative or qualitative risk tolerance and appetite areas seem problematic (flag as red), could be cautionary (flag as yellow), or appear acceptable with no items to report or no action required (flag as green). Some boards and audit committees might only want to see items flagged as red or yellow to avoid information overload—critical due to myriad challenges that many organizations face in today's volatile, global economic environment. Volatility is the new norm in today's business climate and requires a greater need than ever to understand the relationship an organization has in its level of risk appetite and risk tolerance. Correspondingly, this reality also underscores the importance of continuously



## Get the Risk Bundle That Nails It!

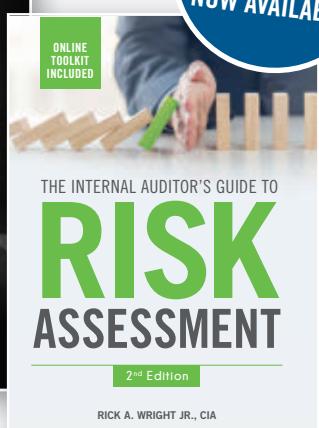
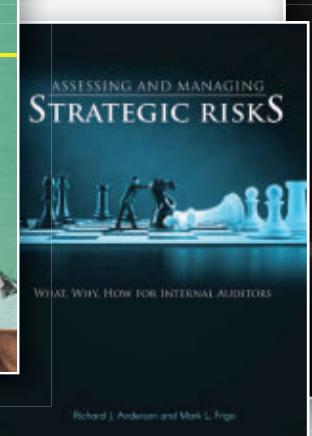
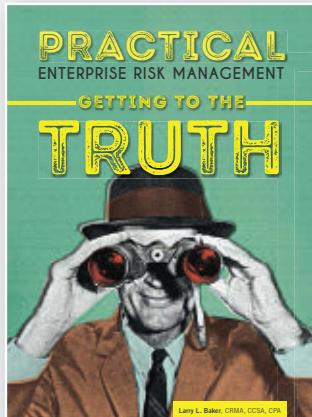
Risk challenges come from every direction. To hit the mark and make sure you're covered from every angle, you must draw from a variety of resources.

The IIA Bookstore's new risk bundle hits the bullseye with four new publications that cover the most pressing issues related to risk.

The bundle is designed to empower practitioners to enhance the value they add to their organizations around risk.

All four titles offer practical, real-world advice to strengthen the risk assessment and management processes and tools to support your efforts.

**Purchase the whole bundle now and **SAVE 10%!****



**BUY YOUR BUNDLE TODAY!**  
Visit [www.theiia.org/RiskBundle](http://www.theiia.org/RiskBundle)



**Bookstore**  
Powered by the Internal Audit Foundation



TO COMMENT on this article,  
EMAIL the author at [sri.ramamoorti@theiia.org](mailto:sri.ramamoorti@theiia.org)

## QUESTIONS FOR INTERNAL AUDIT, EXECUTIVE MANAGEMENT, AND THE BOARD

### Internal audit should consider:

- 1 *Quantitative and qualitative reporting:* As the internal audit department updates or develops its risk assessments of the organization by functional areas against pre-established criteria, do they report the level of risk appetite in both qualitative and quantitative terms?
- 2 *Traffic-light indicators:* Are there indicators reported in the assessment of the levels (red/problematic, yellow/cautionary, green/acceptable) of risk tolerance the organization is accepting?
- 3 *Variability reporting:* Are the levels of risk tolerance being presented in terms of variability? Are these within allowable bands of variation?
- 4 *ERM training adequacy:* Are the levels of training provided for internal audit personnel and for those in governance over risk policies, management, and acceptance processes adequate?

### Management should consider:

- 1 *Enterprisewide risk communications:* Have the organization's strategies and objectives been fully communicated throughout the organization? Has this communication addressed the level of risk tolerance and risk appetite that is considered acceptable?
- 2 *Cross-functional application:* Does management have a cross-functional opportunity to address issues raised by internal audit in its reporting of its assessment of risk tolerance and risk appetite?
- 3 *Scenario analysis:* Does management view risk tolerance and risk appetite assessments using "what if" scenarios to consider business volatility?

### The board and the audit committee should consider:

- 1 *Comprehension of ERM philosophy:* Does the board understand the level of risk tolerance and risk appetite being accepted in the organization and as implemented by management?
- 2 *Board/internal audit relationship:* Does the board have direct input into the level of assessment being performed by internal audit to report its results quantitatively and qualitatively?
- 3 *Responsible and prudent governance:* Is the risk reporting in sufficient detail to allow the board to fulfill its governance responsibilities to address any concerns that could affect organizational stakeholders?



re-evaluating the risk appetite statement in light of changing conditions.

### ENHANCING RISK MANAGEMENT CAPABILITIES

As organizations move aggressively to enhance their risk management capabilities, risk assessments of risk appetite and risk tolerance are going to assume a new and higher level of significance. While risk appetite will always mean different things to different people, a

well-communicated, appropriate risk appetite statement can actively help organizations achieve goals and support sustainability. Clearly, risk management capabilities are evidenced by having disciplined and systematic ways of measuring, calibrating, and responding to risk. In today's environment, such capabilities have become indispensable. Unless internal audit coaches executive management and the board to thoroughly understand the relevance and

importance of the vocabulary around risk and control, organizations will still not have learned real lessons from 2008's financial crisis. <sup>1a</sup>

---

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

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



Drive Your Career Forward  
IIA Certifications and Qualifications

## Shift Into High Gear

Professionals with the Certified Internal Auditor® (CIA®) credential can earn more respect, promotions, and money\* than their peers without a certification.

Begin your quest toward the only globally recognized certification for internal auditors today. Put CIA after your name, and be first on the track for advancement.

---

### The IIA Congratulates the 2017 CIA Exam Award Winners!

#### **William S. Smith Award – Gold**

*(Highest Scoring Candidate)*

Seyed Paul Arab, CIA USA

#### **Kurt Riedener Award – Bronze**

*(3rd Highest Scoring Candidate)*

Wendy Magno, CIA USA

#### **A.J. Hans Spoel Award – Silver**

*(2nd Highest Scoring Candidate)*

Steven Dobberkau, CIA Germany

#### **Dr. Glenn Sumners Award – Student**

*(Highest Scoring Student Candidate)*

Earl O. Jason Gozon, CIA Philippines

Visit [www.theiia.org/TopScoreWinners](http://www.theiia.org/TopScoreWinners) for a complete list of top score winners for all 2017 IIA certifications.

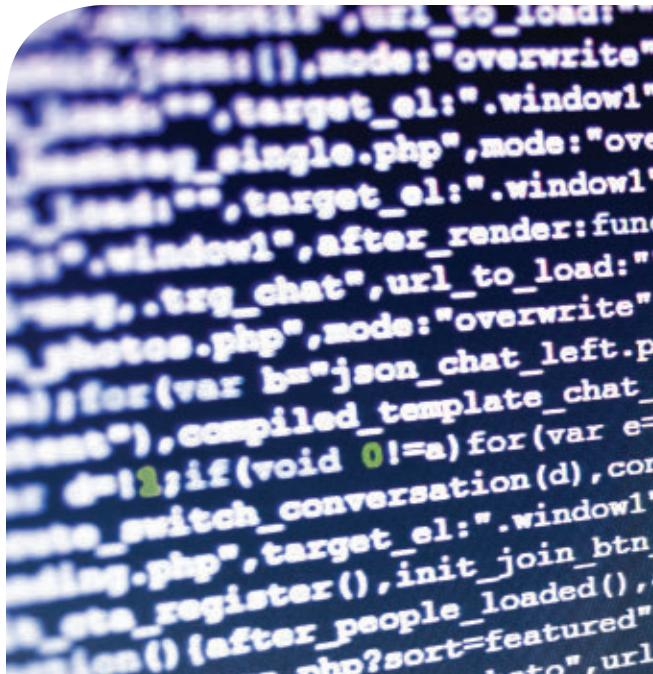
\*Earn on average \$38,000 more annually than those without a certification, according to The IIA's 2017 Internal Audit Compensation Study (based on U.S. responses).

Apply today at  
[www.theiia.org/CIA](http://www.theiia.org/CIA).

The logo for The Institute of Internal Auditors (IIA). It features a stylized globe icon integrated into the letter 'I' of the acronym 'IIA'. To the right of the icon, the words 'The Institute of Internal Auditors' are written in a bold, sans-serif font.

**While organizational analytics can yield powerful insights, they may also be a source of risk.**

**Jane Seago**



```

    "url_to_load": "index.php", mode: "overwrite"
    "target_el": ".window1"
    "script": "single.php", mode: "over
    "target_el": ".window1"
    "script": "single.php", mode: "over
    "target_el": ".window1", after_render: fun
    "script": "chat", url_to_load: "index.php", mode: "overwrit
    "script": "chat_left.p
    "script": "switch_conversation(d), con
    "script": "register()", init_join_bt
    "script": "after_people_loaded()", url
    "script": "sort=featured", url
  
```

# B

usinesses are having a love affair with data analytics. The potential to unlock secrets hidden in the vast quantities of data generated daily makes the technology almost irresistible. And why not? Tools enabling the organization to uncover data patterns that reveal how to implement efficiencies, make better decisions, increase agility, identify untapped market niches, and appeal more viscerally to customers can be extremely valuable.

Internal audit is no stranger to using data analytics to fulfill its responsibilities to the organization. But not only does internal audit use data analytics itself, it also is called on to review the data analytics use of the business units. Such audits are performed because of the growing realization that insights are not alone, hiding in the data; risk lies

# Behind the Data

there as well. And where there is risk, there is a need for internal audit.

"The same types of questions we would consider for other processes in terms of where things could go wrong apply to data as well," says Judi Gonsalves, senior vice president and manager, Corporate Internal Audit, with Liberty



**The same types of questions we would consider for other processes ... apply to data as well.”**

Judi Gonsalves

Mutual Insurance Group in Boston. And with ever-growing volumes of data on hand, and further organizational dependency on that data, those questions become more and more important to ask.

#### ASSESSING THE RISKS

The possibility of things going wrong explains why internal audit should start, if it has not already, reviewing the use of data analytics in the organization. More than 70 percent of chief audit executives (CAEs) surveyed in The IIA Audit Executive Center's 2018 North American Pulse of Internal Audit research indicate that their organization's net residual data analytics risks are "moderate" to "extensive." But what, exactly, are those risks?

A risk cited by several experts can be summed up in the familiar phrase, "garbage in, garbage out." If the data being analyzed is inaccurate, incomplete, unorganized, dated, or siloed, the conclusions drawn from it can hardly serve as the basis for a winning business plan. "We worry most about the completeness and accuracy of the data pulled together and upon which management may

about data quality. "Our audits evaluate the risks around the completeness, accuracy, integrity, and security of data," Rudenko says. "For example, if a data warehouse is part of the data analytics process, we look at risks and controls around the entire path of the data: the sources of the raw data, the methods and technology around transferring the data to the warehouse, the controls over the warehouse, and the transfer to the end user." Rudenko explains that, in this example, if there are errors or problems with the data at any point along this path, then the end result may be flawed and any decisions or conclusions relying on this data may also be flawed. "If there are any weak links along the journey to the end user, then the entire chain may break," he adds.

Alternatively, the data may be sound, but the algorithms used to analyze it flawed. They may contain an ancillary function, such as an edit check, that is doing something other than its intended purpose, without the business unit being aware. This anomaly may not influence the result. But then again, it might.

In addition, questions should be asked about the data collection process itself. Was it ethical? Is the data being used for the purpose for which it was collected? Was it collected in a way to provide objective results or to prove a point?

"We have to be careful of bias in how we, as auditors, test," says Charles Windeknecht, vice president of Internal Audit with Atlas Air Worldwide in Purchase, N.Y. "We cannot let our initial impressions drive our subsequent actions. If we are unduly influenced by an early fact, we may go down an incorrect path, getting a result that appears accurate while not realizing we are unintentionally overlooking other data."

## The more data the organization has, the more incentive it may provide malicious actors to hack into it.

rely," notes Katie Shellabarger, CAE with automotive dealer software and digital marketing firm CDK Global in suburban Chicago. "Management may take the information *prima facie* and not know that the data is wrong."

Tom Rudenko, CAE with online business directory provider Yelp Inc. in San Francisco, echoes this concern

Nearly 75% of CAEs report their organizations' **data analytics** maturity level as less than "established," according to The IIA's 2018 North American Pulse of Internal Audit survey.

## GETTING STARTED

CAEs and internal auditors just beginning to audit the organization's use of data analytics may welcome some words of wisdom to ensure favorable results. The experts offer several suggestions:

- » Consider the advantages and drawbacks to building analytics capability in the existing team versus acquiring talent.
- » Engage with management, especially in the planning process. "If they are not involved, the process may get started, but it is less likely to be sustainable," Rudenko says.
- » Start small. Understand the process and break it into manageable, auditable parts.
- » Have realistic expectations. While the internal audit function may hope to spring from level 1 to level 4 with regard to its ability to use data analytics effectively in the audit process, the reality is that it takes a lot of effort just to go to level 2. The level of internal audit's understanding and capacity to use data analytics does influence how to effectively audit a control process with heavy reliance on similar routines.
- » Take the time to work through the false positives that are likely to arise during the initial execution of the audit testing routines.
- » Look for a win. "Start by auditing candidates, or processes, where you are likely to gain success," Windeknecht advises, "then build on that success."
- » Look to local IIA chapters for shared experience/expertise and libraries of data analytics routines and audits of data-analytics-driven control processes. Some have formed discussion groups specific to data analytics.
- » Have the end game in mind. "Know who is relying on the data and what they are using it for," counsels Robert Berry, executive director of Internal Audit at the University of South Alabama.



If there are any weak links along the journey to the end user, then the entire chain may break."

Tom Rudenko



Management may take the information *prima facie* and not know that the data is wrong."

Katie Shellabarger

Other risks related to data analytics are many and varied. The more data the organization has, the more incentive it may provide malicious actors to hack into it, thus compromising security and privacy. In addition, change management techniques and monitoring/maintenance of who has access to the data are causes for internal audit attention.

## PROVEN METHODOLOGIES

When faced with a diverse and complex range of risks, tried and tested audit approaches often yield the best results. Take, for example, the timing of data analytics-related audits. Windeknecht

indicates that his team's audits are generally driven by the annual plan, which is updated quarterly. "However, if there's a process that's identified as risk-driven, such as analytics, we will audit that process and test those controls as an addition or replacement to the formal plan."

Often, the timing of data analytics reviews depends on the nature of the data. "If the data is critical to the production of our financial statements, then it gets reviewed as part of the ongoing Sarbanes-Oxley process," Rudenko says. "If the data relates to operational, technical, or regulatory risks, the frequency of our

reviews is factored into our audit planning process."

But scheduling is not the only area where established practices can prove beneficial to review of analytics use. The techniques used to conduct the audit can be relatively standard as well. For example, Robert Berry, executive director of Internal Audit

completeness, accuracy, integrity, and security of the data.

- » Processes and controls surrounding the use and security of data are clearly documented and communicated.
- » Appropriate and relevant access and change management controls are in place and tested for operating and design effectiveness.
- » Changes to the control environment and supporting databases are tracked and monitored.
- » The analyses are supported by built-in quality and effectiveness checks to ensure they (and the data) mirror the changes and evolution of the business.

Personnel-related controls are critical in relation to data analytics, particularly management oversight and user education. Shellabarger points out that if users have flexibility to create their own reports/analysis, they need to know how to use the tools correctly and how to evaluate the inputs and outputs. "Essentially, they need to be able to address the completeness and accuracy issues related to using data and tools," she says.

#### THE FINER POINTS

While proven methodologies may come into play throughout the process of auditing the business units' data analytics use, that does not mean such audits do not present their own unique challenges. As with every audit, there are subtleties that must be recognized, understood, and resolved.

For example, Windeknecht points out that even the apparently basic exercise of identifying data analytics is far from straightforward. "What do we define as data analytics?" he asks rhetorically. "Business units are doing analyses in different shapes and forms, using different algorithms and basing



I've seen audit teams reach completely inaccurate conclusions because they went down the wrong path early in testing."

Charles Windeknecht

at the University of South Alabama in Mobile, asks the department he is auditing what reports it generates. "Depending on the source of the data and how it is used, we may need to look at it, because management may be making critical decisions based on it," he says. Berry's team relies on a structured approach to audit the data analytics process and reuses approaches that have worked well in one department for other departments.

A traditional approach applies also to the controls recommended to address any findings: input controls (the data's completeness, accuracy, and reliability), processing controls (reconciliation of changes made to normalize/filter the data), and output controls (accuracy, based on inputs and processes). Consider, for example, the data warehouse, which supports data analytics. It has teams of personnel dedicated to operating and maintaining it, and features pipelines from the sources of data to the warehouse and from the warehouse to the end users. In this scenario, Rudenko suggests assessing whether or not:

- » Personnel have the necessary expertise to ensure the

Nearly all companies say they have implemented big data analysis, are in the process of implementation, or are considering it, according to research and analysis firm Stratecast.

their analyses on different assumptions.” Risks can arise when the internal auditor or the business unit itself incompletely or incorrectly understands or agrees on such foundational issues. “Are the assumptions still valid?” he continues. “How do you perform integrity checks? When was the most recent review of the algorithm? How does one data event influence subsequent activity?”

Internal auditors make a big mistake if they do not validate key assumptions with facts (i.e., confirmation of key data points and the underlying assumptions) before continuing with testing. “I’ve seen audit teams reach completely inaccurate conclusions because they went down the wrong path early in testing,” Windeknecht says. “The root cause for the error was not sufficiently validating assumptions and initial results. The issue is a huge hit to the integrity of the testing and audit process. The issue is not one you want to confront during the reporting phase of the audit.”

Berry points to challenges even in knowing exactly what to audit. He explains, “On a micro level, when you look at a specific department, you have to understand the objectives of the deliverables/reports, the sources of the data, and the distribution of the data.” It is important to review the process undertaken to produce reports: how the data changes through the cycle and how the changes are accounted for. He advises framing the audit around “reconciling base data to final output.”

On a macro level, it is important to prioritize. “Every department has data it is analyzing and using to produce a result, every department has goals and objectives, and every department has to report on how it performs against those goals,” Berry says. “You have to work with the departments to

identify reports used in management’s decision-making process. That will help you know which activities to review and why.”

And, finally, even the most thorough, meticulous audit will fail if its findings cannot be explained in a way that resonates with the business unit that has been audited. Internal auditors must consider the learning modalities of their audit clients when discussing the findings; people hear, see, and experience things differently. While the natural inclination may be to simply hand over a written, text-heavy report, it may be more effective to use visually appealing, concise images in support of the text. A verbal presentation—in support of the written report—that includes concrete examples of the findings or the risks that may accompany the findings is also likely to make a more lasting impression. This gives clients multiple ways to absorb and understand the recommendations, based on the way they process information.

#### MIND THE DETAILS

The old saying that “the devil is in the details” is particularly apt for reviewing data analytics. And, as with



You have to understand the objectives of the deliverables/reports, the sources of the data, the distribution of the data.”

Robert Berry

**Auditors make a big mistake if they do not validate key assumptions with facts before continuing with testing.**

many aspects of internal auditing, a dose of healthy skepticism is helpful. Says Gonsalves: “We cannot assume that just because information comes out of a system, it is automatically correct.” [\[a\]](#)

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



# Elevating team performance

## A European bank CAE shares his five-pronged approach for assessing and developing team members.

In 2010, I became chief audit executive (CAE) of Central Bank of Armenia, an independent institution that oversees and regulates the country's financial sector. During that time, the internal audit department was in a state of flux—the former CAE had been promoted to a board-level role, and many capable internal auditors had left the team. I quickly began reshaping the function by hiring and training new staff members, aligning our methodology to The IIA's International Professional Practices Framework, automating processes, and devising our strategy.

The IIA Practice Guide, *Measuring Internal Audit Effectiveness and Efficiency*, released that same year, prompted me to also start thinking about performance assessment. At the time, Central Bank used a one-size-fits-all approach to measure performance based on the number of planned versus actual hours for tasks—a somewhat bureaucratic activity that added little value. Our department chose to abandon this system in favor of a customized performance assessment approach, triggering a change that soon led the entire organization to follow suit.

My idea was to link performance assessments to staff motivation so that we hire and develop people consistent with our vision of the function. We sought to encompass both short- and long-term objectives and to keep the process simple yet comprehensive. Perhaps more importantly, we aimed to establish what those objectives would mean for individual staff members. With these ideas in

**Ara Chalabyan**



mind, we developed an assessment process—comprising five main elements—that looks to identify and leverage employees' strengths while also determining opportunities for improvement through training, coaching and mentoring, and, most importantly, self-development.

### **DEFINING OBJECTIVES, PERFORMANCE ELEMENTS**

We began by referencing the IIA Practice Guide and other literature on performance assessment to help establish objectives that would satisfy stakeholder needs and provide high-quality work. Our efforts resulted in four main performance objectives:

- » Perform value-adding activity, which is linked to the quality of our recommendations and insights.
- » Successfully execute the annual internal audit plan, where deadlines are met without sacrificing quality.
- » Deliver high-quality reports and documentation, including regular audit reports, summary and other reports, and workpapers.
- » Provide sound and effective communication, both written and oral.

Next, we began thinking about how employee performance would connect to the four objectives. We wanted to help give direction to staff members and motivate them to behave, perform, communicate, and grow in a way that would move toward achieving these objectives. Toward this end, we established five performance elements: collaboration, efficiency, professional development, visibility, and responsibility.

For each of these elements, we devised several measurement criteria. Because every engagement is unique, using simple quantitative criteria—

such as number of risks identified, recommendations given, and open follow-up issues—would have been ineffective. We instead chose primarily qualitative criteria that rely on collective input across the audit function. In other words, everyone contributes to the performance assessment exercise by providing feedback on other members of the team via a questionnaire form and in-person discussion.



#### **Collaboration**

Internal audit performs best when it operates cohesively as a team and leverages collective knowledge, rather than working in silos. As part of our teamwork philosophy, and unlike the rest of the organization, everyone in the internal audit function works together under one roof as a means of facilitating team collaboration.

Per our criteria, an effective collaborator is:

- » *An Active Listener*—participates in discussions and presents opinions.
- » *A Fair-minded Debater*—remains open to debate and separates issues from people.
- » *A Desired Team Member*—someone with whom colleagues would like to work on audit or other projects.
- » *A Supporter*—supports colleagues on both audit-specific assignments and on projects outside his or her primary work responsibilities.

Assessments of collaboration skills are performed as a 360-degree exercise—everyone assesses everyone else anonymously, and generalized results are then discussed with the team. We encourage feedback and stress that

the assessment is meant to serve as a professional development tool rather than a means of punishment. The process also provides an incentive to maintain healthy working relationships across the team, as any self-focused outlier can be identified easily through the assessment. Moreover, all auditors are asked to include the CAE in their assessments, ensuring that everyone, including team leadership, participates in the process.

Maintaining an open and honest environment is key to effective collaboration. The process starts with hiring the right people and continues as we integrate them into the team. Our assessment process then reinforces the importance of collaboration and fosters employee buy-in. And as an added measure, we anonymously select a Knowledge Champion of the Year to promote learning and sharing among the team.



#### **Efficiency**

Auditor efficiency is about delivering quality work to our stakeholders cost-effectively and on time.

We measure efficiency by determining whether our team's practitioners:

- » Provide valuable recommendations both within and outside audit engagements.
- » Meet audit and other project deadlines.
- » Deliver high-quality reports and workpapers.
- » Maintain sound relationships and communication with clients.

These criteria replicate the department's internal audit performance objectives described earlier. Members of the managerial team—composed of the CAE; deputy CAE; and financial, operational, and IT audit unit

# Growth and development opportunities are the top reasons millennials cite for joining an organization, according to The Deloitte Millennial Survey.

managers—discuss staff performance across all four of these areas and provide assessments based on their experience with each individual. They also review self-assessments completed by every team member. Moreover, all staff members provide a peer assessment for those colleagues with whom they worked in the period under review.



## Professional Development

We expect all team members to pursue professional development, even after receiving certifications. With The IIA Global Internal Audit Competency Framework in mind, professional development is defined across four criteria:

- » Interpersonal skills, including verbal and nonverbal communication, listening and negotiation, and teamwork.
- » Technical knowledge and tools, such as data collection and analysis, working with spreadsheets, problem solving, and slide preparation.
- » Knowledge of the *International Standards for the Professional Practice of Internal Auditing*, as well as internal audit theory, methodology, and application.
- » Specialized areas of expertise, such as International Financial Reporting Standards; governance, risk, and control; risk management frameworks; IT auditing; COBIT; and fraud.

We look for each internal auditor to obtain at least one international certification—such as the Certified Internal Auditor (CIA), Chartered Certified Accountant (ACCA), Certified Information Security Auditor (CISA),

Certification in Risk Management Assurance (CRMA), and Certified in Risk and Information Systems Control (CRISC)—relevant to his or her specialty unit and duties. Auditors may pursue other certifications or qualifications from The IIA, ISACA, or the Association of Certified Fraud Examiners. We also consider practitioners' backgrounds—such as whether our financial auditors have Big 4 experience and to what extent our IT auditors possess technology experience.

Development becomes more subtle after someone achieves certification. Evaluation measures include training events attended, presentations delivered, and knowledge and skills developed.



## Visibility

We regard visibility as a key practitioner attribute. Each member of the team should ideally be recognized not only for his or her personal character and ethical behavior, but also for subject matter expertise.

Our assessment criteria for visibility comprise two main areas.

**We look for each internal auditor to obtain at least one international certification relevant to his or her specialty unit and duties.**

First, the internal auditor should be expanding his or her visibility across the organization through participation in bankwide discussions and working groups and by establishing

and maintaining professional relationships with colleagues.

Second, we look for practitioners to expand beyond the boundaries of the organization and become a well-known expert in the industry. This effort may involve volunteering with IIA–Armenia, teaching at local universities or training centers, presenting at conferences, writing articles for professional publications, and serving on audit committees and boards. Further visibility can be obtained by traveling outside the country to speak at conferences, facilitate roundtable discussions, deliver training sessions, and participate in external quality assessment teams. We assess visibility during the period under review against each individual's potential using feedback from colleagues and examining identifiable achievements such as presentations, training engagements, and published articles.



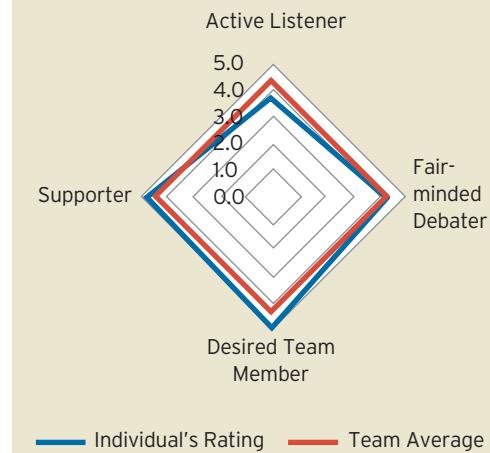
### Responsibility

We measure internal auditors' responsibility by how well they perform their duties.

Responsibility is gauged according to performance on top-down assignments—carrying

## ASSESSMENT RATINGS

**Collaboration Assessment by Quality**



personal initiatives. The latter type of work is important to becoming a true professional and a valued member of the team. Examples include creating a newsletter, developing new training courses, building relationships, and writing articles. However, gaining the ability to perform bottom-up initiatives can take time, especially with new hires, as it often requires extensive knowledge, expertise, and visibility. Some start sooner with small initiatives at the department level, such as developing new designs for presentations, whereas others need more time to begin making bottom-up contributions.

### PROVIDING FEEDBACK

We conduct performance assessments twice a year. And while each follows a rigorous process, the year-end review involves more thorough assessment. Moreover, the collaboration assessments are limited to once annually, to avoid overburdening the team and to allow auditors sufficient time to change behavior if needed.

The managerial team shares feedback directly with each team member

**Gaining the ability to perform bottom-up initiatives can take time, especially with new hires, as it often requires extensive knowledge, expertise, and visibility.**

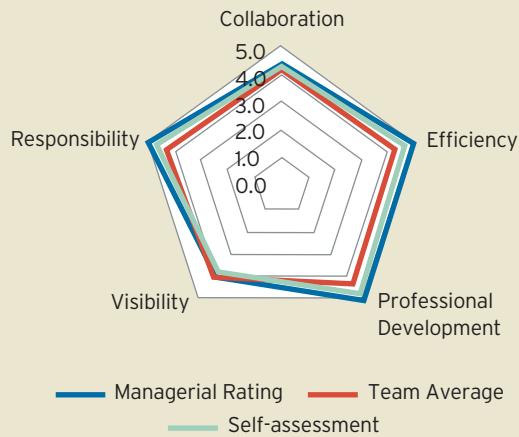
out tasks assigned by audit management—and by work performed from the bottom up, where auditors take additional responsibility through

Professional **development** plans with specific annual targets for **training** help ensure a high level of collective proficiency for the internal audit activity.—IIA 2018 Pulse of Internal Audit survey

**Collaboration Assessment by Assessor  
(Individual Assessors 1-10)**



**Performance Assessment Summary**



via three spider charts. The first two charts depict 360-degree collaboration assessment results, showing the individual's ratings against the average for the four criteria within this measurement (active listener, fair-minded debater, desired team member, supporter) and the average rating for the individual by every assessor against the assessors' average rating for everyone (see "Collaboration Assessment by Quality" and "Collaboration Assessment by Assessor" on page 52).

A third chart shows the individuals' ratings for all five elements of the assessment (see "Performance Assessment Summary Chart" on this page). The chart's blue line represents the managerial average rating, the red line depicts the average for the overall team, and the green line shows the self-assessment.

Our managerial team discusses every element of the assessment with each member of the team. Managers also are assessed. The individual under review is free to join or forgo the discussion. During our most recent assessment exercise, everyone chose to be present at his or her own assessment to

hear positive feedback as well as opportunities for improvement.

Following the year-end assessment, we devise a development plan for each team member for the coming year. The plan includes visibility and initiative strategies, certification goals, and knowledge and skill development through audit engagements where teams are mixed via integrated auditing.

### TANGIBLE RESULTS

Since implementing our assessment process, we've received two "generally conform" ratings from external quality assessments performed by Dutch Central Bank colleagues—one in 2012 and another in 2017—as well as mission-positive conclusions from an International Monetary Fund safeguards assessment. Collectively, our team has a portfolio of numerous certifications, including five CIAs, three CRMAs, four ACCAs, one CISA, and three CRISCs. Several staff members are teaching at local universities and many volunteer for IIA—Armenia by helping organize conferences and other events, developing and maintaining

website content and quarterly bulletins, and promoting membership. Outside the country, some of our staff members have spoken at conferences and other events, delivered training, and participated in external quality assessments.

These results stem from the direction provided by our assessments. We see new team members developing new skills and experienced auditors continuing development beyond certification. Our audit reports receive praise—including best-practice kudos from our external assessors—and relationships with audit clients are balanced. Lastly, our internal auditors are respected as professionals, due in part to their international qualifications and visibility both inside and outside the organization. The assessment process has strengthened our team, expanded its capabilities, and made us an even greater asset to organizational stakeholders. □

**ARA CHALABYAN, CIA, CRMA, CRISC, ACCA,** is chief audit executive at Central Bank of Armenia in Yerevan, and president of IIA—Armenia.

# Relevant. Reliable. Responsive.



## SHARPEN YOUR FOCUS

As the award-winning, multi-platform, always-available resource for internal auditors everywhere, *Internal Auditor* provides insightful content, optimized functionality, and interactive connections to sharpen your focus.

Print | Online | Mobile | Social

+GET it all [InternalAuditor.org](http://InternalAuditor.org)

Ia  
INTERNAL AUDITOR

# Social Capital *Pays Dividends*

**Joshua K. Cieslewicz**  
**Brittany Anderson**  
**Lindsay J.S. Cieslewicz**

To be a trusted advisor, internal auditors need to have strong relationships with executives and audit clients. Building those relationships is about accumulating “social capital.” Social capital is a complex subject with many definitions, but the Social Capital Research & Training website notes that “the commonalities of most definitions of social capital are that they focus on social relations that have productive benefits.” In practical terms, *social capital* refers to the power people are willing to use on another person’s behalf because of the strength of their relationship with that person.

In internal auditing, building and using social capital can mean the difference between successfully igniting change within an organization and just filing another report. Some audit clients perceive that internal audit is at odds with other parts of the organization. They may not think internal audit recommendations are useful and may only make minimal efforts to address them. In addition,

**Relationship building can enable internal auditors to better help audit clients throughout the organization.**

RAWPIXEL.COM / SHUTTERSTOCK.COM



## SOCIAL CAPITAL PAYS DIVIDENDS

clients may use their own social capital to block audit recommendations, support their own positions, or resist meaningful change. Consequently, although internal audit may be in the right, it may not succeed in recommending needed change. This is especially the case when internal audit has not accumulated its own social capital.

However, internal auditors cannot abandon objectivity in pursuit of building relationships. Auditors' ability to balance objectivity and social capital can impact not only what they are able to accomplish, but their career trajectory.

Consider this example: The chief audit executive (CAE) has been asked to join other executives in a luxury box to watch a basketball game. If the CAE participates, is internal audit's independence and objectivity compromised? On the other hand, would choosing to not take part damage the CAE's social capital and compromise internal audit's ability to successfully navigate through challenging issues within the organization?

Attending the basketball game is just one piece of a larger puzzle of interactions between management and internal auditing. If the auditor has already built social capital by demonstrating commitment, being collegial, and proving his or her capabilities, participating in such social events can further the work of internal audit, not cloud it.

### DEMONSTRATE COMMITMENT

While a sense of commitment to an internal auditor's own work is critical, it also is important to consider commitment as viewed through the eyes of audit clients. Successfully initiating change is not just about working hard and delivering an audit report; it is about convincing clients that internal audit has the organization's and the clients' interests in mind. When

an internal auditor seeks to establish common ground, such as the mutual overall goal of improving the organization, the truth can motivate clients instead of frustrate them. For clients, this can mean the difference between feeling chastised and feeling like their efforts to change will be meaningful and worthwhile.

relationship is one of respect rather than of hostility," she says.

This relationship is built on the premise that everyone in the organization—which includes all state departments, agencies, and public universities in Utah—shares a similar commitment. This presumption may not hold true in all cases across

## Successfully initiating change is about convincing clients that internal audit has the organization's and clients' interests in mind.

Interviews with experienced internal auditors reveal how they apply social capital principles to improve audit outcomes. "Everybody involved in an audit has the same goal typically—to make the organization better," says Hollie Andrus, financial audit director for the Office of the State Auditor of Utah. "I am lucky to work with people inside my office and with people I audit who care about their organizations and want to do the best job possible. This certainly makes it easier to create a symbiotic environment."

Building social capital "helps promote change more quickly," she says. "There is a level of respect and trust from both sides of the table, whether that be with co-workers or clients." Andrus' experience shows how emphasizing shared commitment to the organization builds social capital.

However, part of an internal auditor's job is to tackle challenges. Sometimes that means Andrus must write tough findings or recommendations for an audit client. "Organizations receiving these tough findings are more open to our concerns and suggestions if our

such a large organization, but Andrus' attitude and approach invite others to respond in kind.

Establishing shared commitment can be accomplished in many other ways outside of work. One avenue is volunteering for the charitable causes the organization supports. The workplace by necessity has deadlines, pressures, discussions about differences, and sometimes unpleasant interactions. Sometimes volunteering with co-workers, participating on an athletic team, or attending a training conference together builds relationships of trust faster than simply going through everyday business activities.

While such involvement needs to be genuine to build social capital, it is helpful when such involvement is also strategic. For example, Andrus serves on an advisory board of Utah Valley University (UVU), where many of her employees and audit clients received their degrees. Choosing to demonstrate commitment to a university is particularly effective in building social capital because alumni have strong social and emotional ties to their schools. UVU, with Utah's largest student enrollment,

The Organisation for Economic Co-operation and Development defines **social capital** as “networks ... shared norms, values, and understandings that facilitate cooperation within or among groups.”

supports students in pursuing jobs in the state government, so Andrus encounters many graduates in her work. Sharing this common commitment makes building positive work relationships and developing social capital easier than if the shared commitment did not exist.

#### **BE COLLEGIAL**

A willingness to cooperate and be considerate of colleagues builds social capital. If internal audit reports are delivered unexpectedly like knives in the back, objectivity may prevail, but social capital is lost. On the other hand, if there are 10 valid findings and the two most important are watered down after an excellent dinner, objectivity is lost. The better approach is to tackle the big issues, but to do so with collegiality.

J. Michael McGuire, the CEO of Grant Thornton, commented on this issue when fielding questions at an accounting research conference earlier this year. McGuire indicated that the grit and social skills to ask hard questions while maintaining relationships is crucial. He explained that such abilities, or early progress in developing those skills, are among the top characteristics Grant Thornton looks for in new hires and are part of what makes those employees successful.

How do those on the other side of the audit feel about the importance of collegiality? An insurance industry chief financial officer (CFO) explains her perspective on the difference between being audited by a good auditor and a bad auditor. The CFO, who prefers her name not be mentioned, describes a situation in a previous job as a controller that illustrates poor collegiality on the part of an internal auditor.

An internal auditor asked someone in another part of the organization a question and received an

uncertain answer, “I am not sure, but I think....” Rather than verify the employee’s story with the controller, the auditor took the issue up the audit ranks, and his supervisor then approached the organization’s executive team with the issue. When the controller was finally called back into the conversation, she was blindsided with the problem. It turned out there was no problem at all—just misunderstood information.

This story demonstrates that it pays for internal auditors to be collegial with others and show them the respect internal auditors would like to receive, themselves. By neglecting principles of collegiality and failing to confirm the employee’s story with the



**TO COMMENT** on  
this article,  
**EMAIL** the author at  
[joshua.cieslewicz@  
theiia.org](mailto:joshua.cieslewicz@theiia.org)

## **By neglecting principles of collegiality and confirming the employee’s story, the auditor destroyed his social capital in all directions.**

controller, the auditor destroyed his social capital in all directions. The controller lost interest in collegially responding to the auditor’s requests and facilitating a smooth audit. The auditor’s supervisors were frustrated because they had wasted time and frustrated the organization’s executives.

The CFO also describes what it is like to have a collegial internal auditor. This kind of auditor treats audit clients as friends. Everyone knows the auditor’s job still must be done, but being collegial makes the experience less painful. She recommends that auditors think of what it would be like to audit a friend. The auditor would need to inform a friend of mistakes he or she made and of the need to be prompt with information,

but the auditor would do so with decency. This kind of auditor, she says, would be candid, and it would feel as if the auditor is rooting for the client instead of waiting for an opportunity to criticize. Moreover, this auditor would be transparent about where things stand instead of making the client wonder what is happening. This is what a person would do for a friend, because he or she would want to maintain the relationship.

In the CFO's experience, most internal audit clients respond well to

everything, but that he or she prepares as well as possible and admits his or her shortcomings. Otherwise, auditors unnecessarily waste more of the client's time and cause frustration. Paying attention to capabilities can build mutual respect and social capital.

As the organization's employees are impressed with internal auditors' capabilities, they may be more willing to work with them. For instance, the IT function may not want to expose a problem to an internal auditor, but the department may decide to involve

An interesting characteristic of many internal auditors is that even in the midst of their heavy workloads, these practitioners make time and find ways to maintain their social capital. In talking to these professionals, one message becomes clear: They care about people. That caring results in social capital.

### THE SOCIAL CAPITAL APPROACH

Mark Gotberg, assistant director of internal auditing at Brigham Young University, left his previous job at a CPA firm, in part, because he wanted to feel committed to something more important than building others' wealth. This commitment is clear in the contributions he has made to the university. One example has less to do with the results of his audits and more to do with those who work with him. He goes out of his way to hire and train student auditors, and he spends time mentoring students.

In his internal audit position, Gotberg leverages capabilities learned from consulting. When working with his clients, he listens to all levels of employees. He says the people closest to a problem often have the solution to it, but they may not have the ability to put their ideas together, present their ideas, or convince management to apply the solution. "Developing relationships with people at the lowest levels and getting them to trust me has provided me with the best tips for organizational and process improvement," he explains.

Gotberg builds social capital with audit clients as he helps them orchestrate the change they want. His collegiality comes out in this process, as well as in reporting. He makes sure the wording of his reports is as fair and helpful to the client as possible, while always providing the audit service the organization needs. He explores solutions to problems

## If auditors are encouraged to share their strengths with each other, the individual social capital of each auditor and the collective social capital can grow.

collegial treatment. Those who do not may require other approaches. The challenge is to not let the unpleasant experiences keep internal auditors from building social capital with those who are more amenable.

Joni Lusty, an assistant director at EY, has experience recruiting and developing employees in all areas of the business. Her simple and practical recommendations for building social capital center around collegiality. First, it is best to be oneself, and to be honest and straightforward. Second, she recommends listening carefully to avoid jumping to conclusions and making assumptions about what people are saying. When clients feel that internal auditors are doing this, they are more likely to do the same with the auditor.

### LEVERAGE CAPABILITIES

In internal auditing, capability does not mean that the auditor knows

internal audit if it has worked with the auditor before and seen how he or she solves problems.

Although it is challenging to be all things to all parts of an organization, internal audit's usefulness can increase when the team comprises people with strong but different skills. If auditors are then encouraged to come to each other's aid and share their strengths with each other, the individual social capital of each auditor and the collective social capital can grow. This can enhance the group's overall ability to work together and help the organization improve.

Often, CAEs and internal audit partners in audit firms are respected for the skills they have developed over time. Those capabilities include a mixture of analytical and soft skills. These people are usually well-connected to many other professionals because of their adherence to principles of relationship building.

**26%** of internal audit respondents say they are **experts** at building relationships and **39%** are advanced, according to The IIA's 2015 Common Body of Knowledge Internal Audit Practitioner Survey.

and manages clients' expectations. By using these skills, he builds social capital instead of just finishing audits and producing reports.

Andrus also comments on this social capital-focused approach to internal auditing. "Adversarial relationships only breed dislike and hostility—nothing is accomplished and nothing is improved upon," she says. "An audit client once told me that he would make corrections I proposed because of my attitude toward the audit and the client. He also said that if another auditor—one who was more hostile—requested or proposed the same changes, he would 'dig his heels in' and would not make the change because of the other auditor's attitude." Giving credence to social capital in the right ways can enhance

an internal auditor's effectiveness rather than subtract from it.

#### A SOCIAL INVESTMENT

In the balancing act between objectivity and developing relationships, it is not always possible to build social capital with audit clients. For instance, sometimes internal auditors prepare cases and assist in prosecutions. As difficult as this type of situation may be, it also can highlight internal auditors' capabilities and make clear their commitment and efforts to accomplish the organization's goals. This, in turn, can impress the right kind of people in the organization and build social capital with them.

Reconsider the question of whether the CAE should accept the invitation to attend the basketball

game with the other executives. The answer is "yes," if the CAE has carefully built the right kinds of relationships through demonstrating commitment, being collegial, and leveraging internal audit's capabilities to deliver worthwhile results. The social capital created at the event may be helpful when a future daunting issue requires cooperation from audit clients. Social capital, then, is like money in the bank—develop it now because internal auditors eventually will need it. □

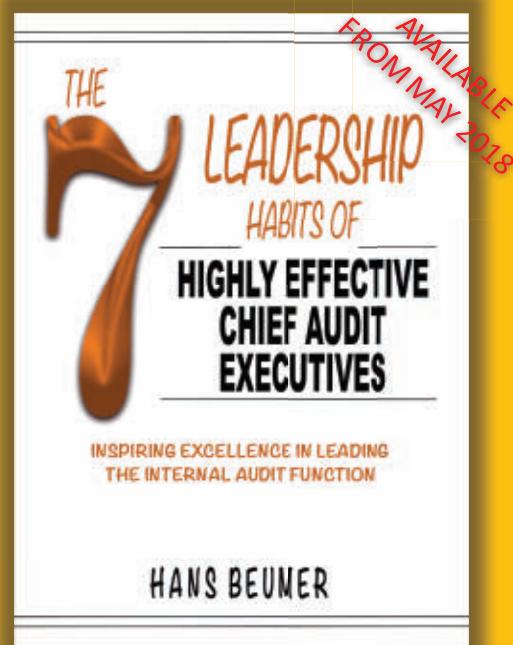
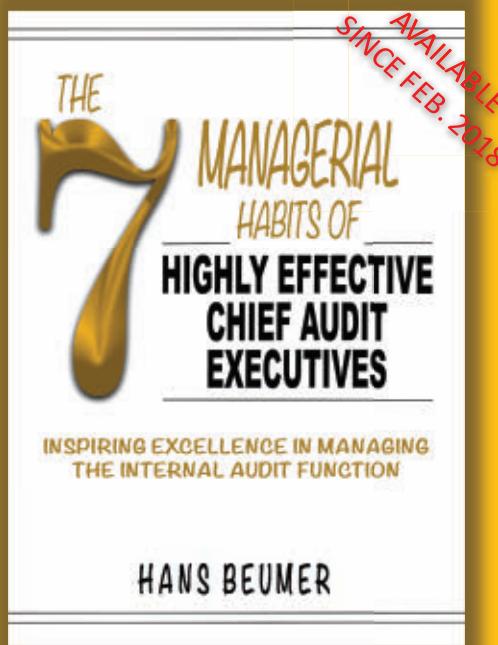
---

**JOSHUA K. CIESLEWICZ, PHD, CPA,** is an associate professor of accounting at Utah Valley University in Orem.

**BRITTANY ANDERSON** is an associate auditor at PwC in San Jose, Calif.

**LINDSY J.S. CIESLEWICZ** is a writer based in Orem, Utah.

## NEW BOOKS – INSPIRING EXCELLENCE IN MANAGING AND LEADING



Available in Print and EBook, at the IIA Bookstore, [www.theiia.org/Bookstore](http://www.theiia.org/Bookstore) or Lulu, Amazon, iBook Store, Barnes Noble, Ingram

# Governance Perspectives

BY KAYLA FLANDERS

## AN APPETITE FOR RISK

Internal audit departments may need to recalibrate to accept more risk.

It is a time of great change in internal auditing, and the expectations to deliver have never been higher. There are many new—and some repackaged—concepts floating around, such as audit innovation, agile auditing, becoming a trusted advisor, and strategic auditing. One thing that has not changed, however, is internal audit's desire to add value to the organization through the execution of its work, whether through assurance or consulting activities. Internal audit, more than ever, is moving into areas of the business—such as strategic planning and culture—that are more subjective and require more auditor judgment. Venturing into these areas may require auditors to recalibrate their risk appetite and accept more risk going forward.

To successfully meet the expectations of their key stakeholders, chief audit executives (CAEs) must first

ensure that, foundationally, internal audit is set up for success. A key element is that the objectives of the internal audit department are clearly defined and agreed upon with stakeholders, and an assessment of the risks to achieving those objectives are clearly identified. Building the elements of risk management into the day-to-day activities of internal audit, from the overall operations of the department down to the engagement level, will ensure sustainable activity and should facilitate more agile auditing through clear understanding of risk appetites and tolerances.

Internal auditors, while having the unique position and ability to provide opinion on the ability of others to identify and manage risk, whether strategic, operational, compliance, or financial, seem less inclined to look internally at their own risk management practices. Internal audit's appetite for

risk may be too low, inhibiting agility, innovation, and the transformation of the function. Although there is no absolute assurance in internal auditing, it is easy to default to a risk-averse position when headlines call out internal audit specifically—Where were the auditors?—when analyzing compliance failures, cultural issues, and material weaknesses or significant deficiencies in internal control over financial reporting.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) updated *Enterprise Risk Management—Integrating With Strategy and Performance* provides the opportunity to take a fresh look not only at the organization's risk management practices, but also those within internal audit. Although it is directed at the enterprise level, the updated framework is scalable, and parallels can be drawn to the department or function level.

**READ MORE ON GOVERNANCE** Visit [InternalAuditor.org/governance](http://InternalAuditor.org/governance)



TO COMMENT on this article,  
EMAIL the author at [kayla.flanders@theiia.org](mailto:kayla.flanders@theiia.org)

When looking at risk management within internal audit, CAEs can follow the model that the framework has established, starting with the mission, vision, and core values of the department and ending with the delivery of enhanced value through its risk management processes.

**Step 1 - Mission, Vision, and Core Values** Internal audit should clearly articulate its mission, vision, and core values. It should start with The IIA's Definition of Internal Auditing and then survey key stakeholders to understand the expectations of the internal audit department. The mission and vision will vary by organization depending on many elements, including the industry, how highly regulated the entity is, and the overall governance structure. The mission and vision may be aspirational depending on the level of maturity of the internal audit function. The steps to achieve an aspirational mission and vision may be part of the risk profile.

The new COSO framework clearly indicates that a key component of sustainable and embedded risk management is to align with strategic objectives. The mission, vision, and core values are the foundation for the strategy, business objectives, and performance. Managing the risks associated with those items will drive enhanced performance.

**Step 2 - Define Strategy and Identify Business and Performance Objectives** In identifying internal audit's business and performance objectives, there should be alignment to the organization's overall objectives and consideration of the feedback received from key stakeholders. For example, a proposed internal audit strategy could be that the function should primarily focus on compliance-related audits. The objective could be to ensure that the first—and second, if applicable—line of defense have appropriate risk management and internal controls in place to address compliance-related risk. A risk implication of this strategy is that other risks are not covered by internal audit, as the strategy is too narrow. That risk (although not recommended) could be accepted by the appropriate stakeholder based on the governance structure in place. Clearly defining the audit strategy, and related business objectives and performance, should help facilitate audit operations and the audit plan, with all stakeholders aligned on what falls under internal audit's purview.

**Step 3 - Identify the Risks, Risk Appetite, Risk Tolerance, and Risk Response** Internal audit should identify the risks of not achieving the determined audit strategy and business and performance objectives. For each risk, internal audit should consider its risk appetite, tolerance, and

response. For example, a risk to performance of the audit plan may be lack of personnel with technical expertise in specific subject matters. The risk appetite for this situation may be relatively low, to comply with the *International Standards for the Professional Practice of Internal Auditing's* Standard 2230: Engagement Resource Allocation. The risk tolerance may be limited, and the likelihood of the risk occurring may be high, depending on the department make-up and audit universe. Appropriate risk responses include accept, avoid, pursue, reduce, or share. Internal audit may choose to share this risk by co-sourcing resources within the organization (as appropriate, considering independence and objectivity restrictions) or with an external subject-matter expert.

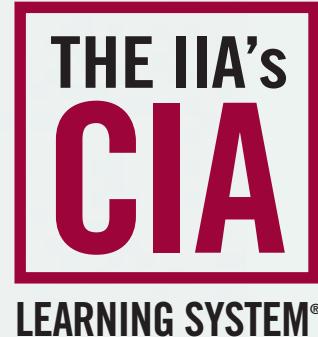
**Step 4 - Stakeholder Buy-in** Throughout the various phases of the process, the CAE should work with key stakeholders to ensure buy-in with the finalized elements, as there is a cascading effect from the determination of the mission and vision; through the strategy, objectives, and performance; to the determination of relevant risks and the risk appetites, tolerances, and responses. The governing body, typically the audit committee, should have the final authority in concurring with the risk responses, especially when the risks are accepted.

As the internal audit risks are built out, with defined risk appetites, tolerances, and responses, this information should be distributed throughout the department to educate team members on expectations and enable them to use it to make risk-based decisions when executing audits. Defining authorities around risk decisions throughout the framework will empower the different levels within audit to make judgment calls and use critical thinking to complete audits in the most agile way.

Risk management should not be a once-a-year process, but instead continuous and evolving as necessary based on risk changes at the organizational level and within the internal audit department. The process and framework should be pliant enough to flex and pivot as needed, with clearly defined governance processes around when specific stakeholders from senior management to the audit committee need to authorize or review changes. Understanding internal audit's strategy and objectives, defining the risks to achieving them, and adding a new level of transparency to risk responses should facilitate internal audit's transformation into a trusted advisor and demonstrate the most effective use of its resources in creating and preserving value. [\[a\]](#)

---

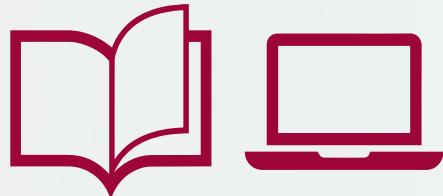
**KAYLA FLANDERS, CIA, CRMA**, is senior audit manager at Pella Corp. in Pella, Iowa.



# 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](http://www.LearnCIA.com)





TO COMMENT on this article,  
EMAIL the author at [michael.jacka@theia.org](mailto:michael.jacka@theia.org)



BY J. MICHAEL JACKA

# THE BORING AUDIT DEPARTMENT

Predictable audits that stick to the script and play it safe provide little value to stakeholders.

Austin Kleon, a self-described “author who draws,” recently wrote that he believes people behave as if they have a secret wish to be bored to death. As he explains in a blog post, Kleon imagines people saying, “I want artists to say all the right things. ... I want artists to play it safe. I want me and my artists to be best friends forever. I want artists to do and be all of these things and then I want to be allowed to complain how boring art is.”

I have always believed that internal audit work is more art than science. Take the audit report. I worked with someone who saw electronic workpapers as the answer to all his report-writing woes. In every meeting about improving either our reports or our workpaper system, he would arrive with suggestions on how to reduce reports to a collection of pull-down menus and buttons—all designed to remove human error from the process. He never said the words, but what he wanted was a fill-in-the-blanks audit report.

Effective audit reports are not a collection of stock phrases and plugged-in data; they are an artfully constructed blend of perfected verbiage, salient points, and appropriate support—all balanced to represent the needs of both internal audit and its stakeholders. Effective report construction is an art.

Likewise, effective completion of an audit project is also an art. And ultimately, the development and maintenance of an effective internal audit department is an art.

With that in mind, reread the quote from Kleon. But this time, whenever the word *art* appears, replace it with the phrase *internal audit*.

Many board members, executive managers, and even internal audit leaders don’t want anything extraordinary from their audit departments—nothing challenging, nothing outside the box, nothing that might ruffle feathers. They want internal audit to stick to the script, remain predictable, and play it safe at all times. Not surprisingly, these same

individuals are among the first to complain they are not getting anything from their internal audit departments—they say that it provides no value, that it represents a drain on the organization, that it is, dare we say, boring.

We accede to their desires at our own peril. If we avoid excitement, if we avoid confrontation, if we avoid the unpredictable, if we avoid risk, and if we worry about maintaining friendships, then we forfeit our right to complain about the results. The minute we think we can fill in the blanks, keep repeating what we’ve done in the past, and survive by sticking with the status quo is the minute we inevitably become boring.

And if we make internal audit boring, we have no one to blame but ourselves for our ultimate demise. No one needs a boring audit department. *[a]*

---

**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](http://InternalAuditor.org/mike-jacka)

# Eye on Business

## CRAFTING THE AUDIT REPORT

Understanding stakeholder expectations is key to internal audit reporting.



**MICHELLE HUBLE**  
Partner, Internal Audit,  
Compliance and Risk  
Management Solutions  
PwC



**SANDY PUNDMANN**  
U.S. Internal Audit  
leader, Risk and  
Financial Advisory  
Deloitte

### What are internal auditors doing wrong with audit reports?

**HUBLE** Internal audit reporting often is not part of a broader stakeholder communication plan. Before internal auditors determine their approach for audit reports, they should understand the various internal audit stakeholder expectations and establish a plan for formal and informal communication. As report preferences will vary by organization, and even individual, having a comprehensive reporting plan will ensure internal audit is communicating the right information, in the right format, at the right time. Specifically, internal auditors commonly create very long reports with a lot of context their particular readers may not find valuable. This makes finding the important information difficult, or it is potentially missed altogether. Internal auditors can use other forms

of reporting, including verbal communication and memos, for smaller groups of recipients.

**PUNDMANN** Internal auditors sometimes issue audit reports that look more like workpapers, with lots of words and data, providing few—if any—relevant insights and action items. If internal auditors really want to be seen as adding value to their stakeholders, they need to start reporting more strategically, with information relevant to the reader, leading with insights and action items instead of data.

### What is often missing from the audit report?

**PUNDMANN** Audit reports are often missing the “why does this matter?” aspect. Auditors diligently try to write their findings using the condition, cause, criteria, and effect format. But, many times they don’t convey the risks or opportunities, which tell readers why they should

care. Formatting also is key. Can readers easily scan the report to quickly get the information they need? Does the report include an executive summary, key insights, and graphics? Audit reports should provide perspectives on what the project did not cover to avoid offering a false sense of security. For example, a cyber audit could mean many different things to different stakeholders.

Did you conduct an attack and penetration audit? Did you look at resiliency? Clarifying which areas were in and out of scope can prevent the false comfort that comes with assuming auditors assessed something.

**HUBLE** Insight! Internal auditors can demonstrate the most value when they translate their internal audit results—observations as well as leading practices—into meaningful information from a business perspective. Internal auditors should ask themselves “So what?”

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



TO COMMENT on this article,  
EMAIL the author at [editor@theiia.org](mailto:editor@theiia.org)

when drafting the first paragraph of the audit report. They should think from a business leader perspective and communicate in a way that enables the business to understand the connection of the audit report to the business operation and to achieving its strategic objectives. Internal auditors also need to apply professional judgment and be comfortable giving insight on overall control environments without testing the entire control set within a particular function or process. By clearly articulating the scope of the audit, risk priorities, and their assessment of management's control awareness, internal auditors can apply their business acumen and provide insight from audit results that go beyond the number of control weaknesses identified.

#### **What should auditors leave out of the report?**

**HUBLE** Information that has no correlation to the risks deemed as high priority in the risk assessment. Often, we see internal auditors performing end-to-end audits over an entire department or process, testing controls that pertain to risks that are not seen as a priority for the organization. I've seen where low issues are not included in an audit report, though I would caution if an audit plan is truly risk driven, these issues should still be worthy of written documentation. I suggest auditors evaluate, during the

used to provide supporting data and facts for the reader who wants more information. Exclude extraneous words and data that don't add value to the report. How many audit findings start out with "During our review we noted that ..." Filler words take away from the far more important insights elsewhere in the report. Crispness is key.

#### **What types of visuals can enhance an audit report?**

**PUNDMANN** Lengthy reports that don't call attention up front to the most important items miss an opportunity to effectively communicate with the reader. Stakeholders want a quick view of priority areas first to help them get context and perspective, so they can discern where they need to dig in more deeply. Those quick views could come in the form of graphics, charts, infographics, ratings, or dashboards. We've particularly seen dashboards work well by offering visualizations or heat maps of internal audit assessment areas.

**HUBLE** Charts are always a favorite, as they are quick and easy to gauge results from a comparison of data. I suggest internal auditors start using interactive dashboards to further reinforce the notion that reporting is one piece of ongoing communication. Through interactive dashboards, report recipients can navigate the information and ask questions, allowing them to consume the information in a customized, organic way.

## Audit should align its communication plan with the organization's overall digital transformation.—*Michelle Hubble*

audit planning phase, what control activities are correlated to priority risks and the overall audit objective. Continuing to consider the "so what" factor, the auditor will sharpen the audit scope. This way the auditor not only avoids documenting information that is not pertinent to the audit objective, but also does not spend time testing these areas. The level of detail for testing and reporting is something leading practice internal audit functions discuss with their stakeholders, explicitly with the audit committee or governing body. As reporting is a function of the assurance provided, it is essential that the auditors include or omit information as aligned with the internal audit mandate and risk assessment and audit plan approach.

**PUNDMANN** Auditors don't need to share the entire journey of how they arrived at a finding. Appendixes can be

#### **Are there any adjustments for audit reports that will be read on smartphones?**

**HUBLE** Regardless of how a report is viewed, internal auditors should consider how the reader will consume the information. Of course, reports will be read on smartphones and format-

ting needs to be considered. Internal audit should align its communication plan with the organization's overall digital transformation—a strategic initiative in many organizations—specifically, as organizations shift to using apps in place of smartphone enabled, web-friendly browser views. Internal audit should lead by example and consider how it can communicate through a more holistic digital channel, such as using apps to communicate and interact across the function and with its stakeholders.

**PUNDMANN** We need to assume that all audit reports will be read on a smart device. Beyond putting those reports in a device-friendly format, internal audit should try to get its key messages across up front in an executive summary or in the body of an email without forcing the reader to open endless attachments. **[a]**

## IIA Training Stations

TRAINER	PLATFORM	ON-TIME
IIA ONDEMAND		24/07
IIA ON-SITE		09 TO 05
IIA IN-PERSON		09 TO 05
IIA 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](http://www.theiia.org/Training)



ONDEMAND / ON-SITE / IN-PERSON / ONLINE

# IIA Calendar



## IIA CONFERENCES

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

**MAY 6-9**  
**International Conference**  
Dubai World Trade Centre  
Dubai, UAE

**AUG. 13-15**  
**Governance, Risk & Control Conference**  
Omni Hotel  
Nashville, TN

**OCT. 1-2**  
**Financial Services Exchange**  
Renaissance Downtown  
Washington, D.C.

**OCT. 3**  
**Women in Internal Audit Leadership Forum**  
Renaissance Downtown  
Washington, D.C.

**OCT. 3-4**  
**Environmental, Health & Safety Exchange**  
Renaissance Downtown  
Washington, D.C.

**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](http://www.theiia.org/training)

**APRIL 3-12**  
**Assessing Risk: Ensuring Internal Audit's Value**  
Online

**APRIL 3-26**  
**CIA Learning System Comprehensive Instructor-led Course – Part 2**  
Online

**APRIL 9-18**  
**Risk-based Auditing: A Value-add Proposition**  
Online

**APRIL 10-13**  
**Various Courses**  
New York

**APRIL 16-25**  
**Performing an Effective Quality Assessment**  
Online

**APRIL 17-26**  
**Lean Six Sigma Tools for Internal Audit Fieldwork**  
Online

**APRIL 24-27**  
**Various Courses**  
Chicago

**APRIL 30-MAY 3**  
**Various Courses**  
Las Vegas

**MAY 1-10**  
**Audit Report Writing**  
Online

**MAY 1-10**  
**Fundamentals of IT Auditing**  
Online

**MAY 2-18**  
**Various Courses**  
Lake Mary, FL

**MAY 7-9**  
**Auditing Security Monitoring**  
Online

**MAY 8-11**  
**Various Courses**  
Washington, D.C.

**MAY 14-23**  
**Cybersecurity Auditing in an Unsecure World**  
Online

**MAY 14-23**  
**Operational Auditing: Influencing Positive Change**  
Online

**MAY 15-18**  
**Various Courses**  
San Francisco

**MAY 15-24**  
**Lean Six Sigma Tools for Internal Audit Planning**  
Online

**MAY 24**  
**Fundamentals of Internal Auditing**  
Online

**JUNE 4-22**  
**CIA Learning System Comprehensive Instructor-led Course – Part 1**  
Online

**JUNE 5-8**  
**Various Courses**  
Dallas



BY SETH PETERSON

## EMBRACE CHANGE OR BECOME OBSOLETE

Internal auditors must grasp technological innovations and continually seek to evolve.

Innovative, disruptive technology represents a key focus for today's organizations. With increasing regularity, we hear about a new technological advancement that will completely change the way businesses, and even internal audit functions, operate. And while some auditors welcome these developments, others shy away from them, often worrying how the technology could affect their work. But we have become accustomed to adapting to the business environment and using it to showcase our value. In fact, adaptation is not just an important part of our work—it's a professional imperative. Internal auditors must embrace and leverage technological innovations, or risk becoming obsolete.

Neglecting to familiarize ourselves with new technologies impacting organizations will cause us to fall behind and become less relevant to stakeholders. Internal auditors cannot possibly provide meaningful assurance or add value if we don't keep up with the latest developments and factor them into our work. There is no shortage of information available on

topics such as artificial intelligence (AI) and blockchain, and there is no excuse for neglecting to research them. Not only do we shortchange our clients by ignoring these areas, but we also cannot make the technologies work for us without first understanding their capabilities and potential applications.

Ignorance of technological change prevents internal auditors from leveraging innovative tools as multipliers of capacity. While AI will almost certainly eliminate some jobs, the Gartner Research report Predicts 2018: AI and the Future of Work forecasts a net jobs increase due to AI by 2020. Imagine a situation where manual and tedious internal audit tasks are automated, allowing practitioners to focus on driving real value to the organization. While this scenario only scratches the surface of what may be possible with AI, it illustrates the powerful, multiplying effect of using the technology.

Ultimately, neglecting to grasp and absorb technological change is a disservice to ourselves, the organization, and the profession. The IIA has taken a clear stance on

professional development through Standard 1230: "Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development." There is no better skill to develop than one that will ensure the future relevancy of our profession.

For internal auditors to genuinely embrace technology and leverage its potential multiplying effect, we must act without fear to understand the possibilities, keep an open mind, and continually evolve. But at the same time, technological advances should never be used to replace our skills—they should augment them. As always, the skills that will set auditors apart in the digital age will be the ability to think critically and communicate clearly. The most successful future audit leaders will be those who can understand and leverage technological change, as well as clearly articulate its potential impact to stakeholders. **la**

---

**SETH PETERSON, CIA, CRMA, QIAL,** is vice president, internal audit manager, at *The First National Bank in Sioux Falls, S.D.*

READ MORE OPINIONS ON THE PROFESSION visit our Voices section at [InternalAuditor.org](http://InternalAuditor.org)



# Thank You for Making 2017 a Success!

Through support from individuals, organizations, and IIA chapters and affiliates, your contributions allow the Internal Audit Foundation to continue to advance the profession through knowledge and education.

## Foundation Strategic Partners



## Foundation Partners



Support Our Vision and Mission.  
Make Your Donation Today!  
[www.theiia.org/Foundation](http://www.theiia.org/Foundation)

## Diamond Partners (\$25,000+)



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

## Platinum Partner (\$15,000 – \$24,999)

IIA–Philadelphia Chapter

## Gold Partners (\$5,000 – \$14,999)

ExxonMobil Corporation

IIA–Detroit Chapter

IIA–San Francisco Chapter

IIA–Toronto Chapter

The Estate of Wayne G. Moore, CIA

The Vanguard Group





## Are you ready for the future of internal audit?

Assure. Advise. Anticipate.

As organizations push the bounds of disruption, internal audit functions are evolving their approaches to not only deliver assurance to stakeholders, but to advise on critical business issues and better anticipate risk. Through custom labs, we can help you develop a strategy to modernize your Internal Audit program, tapping into the power of analytics and process automation; enhance your Cyber IT Internal Audit program; and incorporate Agile Internal Audit to keep up with the rapid pace of change.

**[www.deloitte.com/us/ia-future](http://www.deloitte.com/us/ia-future)**