

# Ia

INTERNAL AUDITOR

FEBRUARY 2020

A PUBLICATION OF THE IIA

Managing Regulatory Change

The Internal Audit Skills Mix

Intelligent Risk-taking at the  
Canada Revenue Agency

A Sound Strategy for  
Assessing AI Risks



## A VOICE IN THE BOARDROOM

For internal auditors who build  
credibility with the board, opportunities  
to add value have never been greater.


In this data-driven world, is trust the hardest thing to build?

[ey.com](https://ey.com) #BetterQuestions



The better the question. The better the answer.  
The better the world works.





“My CIA sets me apart from  
my peers and shows that  
I can make a difference.”

Ahmed Bassiouni, CIA, QIAL  
United Arab Emirates  
*CIA Since 2009*

**CIA Proves Credibility and Proficiency.**  
Get started today at [www.theiia.org/CIA](http://www.theiia.org/CIA).





## IIA Training Stations

IIA ONDEMAND

# Learn From The Leader.

IIA TRAINING ONDEMAND  
PLATFORM OPEN 24/7

Featuring a suite of on-demand courses that tackle emerging issues and challenges, IIA Training OnDemand provides convenient, self-paced, and cost-effective professional development; accessible online, anytime. With an expanded training catalog, you can easily earn the CPEs needed to stay on the leading edge of the internal audit profession's best practices and proven techniques.

Get On Board. [www.theiia.org/OnDemand](http://www.theiia.org/OnDemand)

 The Institute of  
Internal Auditors





## F E A T U R E S

**24 COVER A Voice in the Boardroom** Board members and audit executives weigh in on the best path to ensuring internal audit is heard by corporate directors. **BY ARTHUR PIPER**

**31 A Plan for Regulatory Change** A top-down assessment model can help internal auditors keep tabs on regulations and ensure the organization is prepared for what lies ahead. **BY NANCY HAIG**

**36 Forming Today's Internal Audit Function** Audit leaders must make sure their teams have the right skills to serve their organizations effectively. **BY RUSSELL A. JACKSON**

**41 A Study in Risk Tolerance** The Canada Revenue Agency is seeing benefits from its pilot of a tool to measure risk exposure versus

organizational tolerance. **BY LOUIS SEABROOKE AND AMY FELIX**

**46 Bringing Clarity to the Foggy World of AI** Strategy and governance should be internal audit's focus in assessing artificial intelligence systems. **BY KEVIN M. ALVERO AND WADE CASSELS**

**51 On the Money: Time to Revisit Financial Risk** Against a backdrop of an over-leveraged economy, there is increased impetus for internal audit to assess financial risk. **BY BRENDAN SCOTT**



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

# Go Audit. And Beyond.

Free yourself from the chains of disconnected spreadsheets, antiquated GRC systems, and makeshift audit software.

Designed for auditors by auditors, AuditBoard's top-rated audit platform unlocks your team's potential, helping you take Audit's strategic value to places beyond.



Request a demo at [auditboard.com/demo](https://auditboard.com/demo)

Top Rated Audit Software On



## DEPARTMENTS



**7 Editor's Note**

**8 Reader Forum**

**63 Calendar**

### PRACTICES

**10 Update** Culture and talent are top 2020 concerns; COSO releases cyber guidance; and AI proves difficult to deploy.

**14 Back to Basics** Is it better to specialize or generalize?

**16 ITAudit** Auditors need to be aware of the risks that accompany RPA.

**20 Risk Watch** Executive sessions can enhance the organization's risk culture.

**22 Fraud Findings** A cost-savings initiative hides a \$15 million fraud.

### INSIGHTS

**56 Board Perspectives** Boards should have a process for overseeing whistleblower allegations.

**59 The Mind of Jacka** Auditors need to let the work lead them to where they least expect.

**60 Eye on Business** Talent management should evolve with the organization.

**64 In My Opinion** Asking why is key to understanding the organization.

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



**Where There's Smoke There's Not Always Fire** Even the most startling anomalies found during audits can have a legitimate explanation. It's imperative to avoid rushing to judgment.

**An Evolving Profession** IIA President and CEO Richard Chambers discusses where internal auditing has been and what challenges and opportunities he sees on the horizon.

**Privacy Law Puts California Consumers in Control** The California Consumer Privacy Act poses big compliance risks for businesses that gather and sell residents' personal data.

**An Education in Misleading Ads** U.S. regulators have many options for investigating deceptive advertising and marketing claims made by universities.





# GAM

WHERE LEADERS EVOLVE.

March 16–18, 2020

ARIA RESORT & CASINO | LAS VEGAS, NV

---

***REGISTER NOW!***

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







## ENJOY THE RIDE

**N**o profession stays the same. If it doesn't evolve, it doesn't survive. In today's changing business world, continuous skills development is key to succeeding. Professionals need to hold on tight, as keeping skills current can be a dizzying ride.

Take magazine publishing, for example. Last week, I interviewed IIA President and CEO Richard Chambers for a video for [InternalAuditor.org](http://InternalAuditor.org). Ten years ago, hosting a video would not have been part of my job description. Once solely a print-based industry, magazine publishing has transformed into a mix of print and digital to address the many ways readers consume content. Digital magazine publishing requires a different set of editing skills, as well as knowledge of apps, video, podcasts, etc. From someone who is evolving with the profession, it has been, and continues to be, a fun and challenging experience.

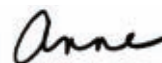
The same can be said about the internal audit profession. Once a profession of ticks and ties, today's internal auditors are consultants and advisors to their organizations on topics ranging from strategy to cybersecurity. Their required skills have grown immensely. "There is a redefinition of capabilities grounded in three dimensions: business acumen, analytics acumen, and technology acumen," says Mike Maali, a partner at PwC, in "Forming Today's Internal Audit Function" (page 36).

In the same article, author Russell Jackson compares staffing internal audit with all of those requisite capabilities to solving a Rubik's Cube. "But just as a Rubik's Cube can be solved, there is a solution for internal audit department staffing," he writes.

According to Chambers, focusing on the gaps is the start of that solution. "What it really involves is constantly looking at your capabilities as an internal audit department compared with the risks that the organization faces and the demands that are being placed on it," he says in our recent [InternalAuditor.org](http://InternalAuditor.org) video interview. He tells me departments then need to develop talent internally or come up with a good sourcing strategy to address the gaps.

That strategy could involve *gig* employees, temporary hires brought on for a project or to address a specific short- or long-term need, or some other limited solution. "We're seeing more organizations using rotational or guest auditor programs to engage professionals with diverse areas of expertise outside of internal audit to help address the varied challenges that core internal audit work presents," says Sandy Pundmann, U.S. internal audit leader at Deloitte, in "Eye on Business" (page 60).

This issue is chock-full of advice from experts on how audit functions and internal auditors can grow and expand their knowledge to thrive in today's business environment. As in other professions, it's a challenging proposition. My advice? Enjoy the ride.



@AMillage on Twitter

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



the misfortune of finding themselves in this unpleasant and sad situation. It is disheartening to see that those of us who dare to be brave are the ones who end up losing our jobs, and possibly careers. But like Norman, I would not have it any other way, and I walk away from my role, and possibly career, with pride, knowing that I did my job professionally and with integrity. It's the most important reason why we're in this profession after all.

**TERESA KIU** comments on Norman Marks' "Internal Auditors Should Be Brave" (December 2019).

## Internal Audit's Story

The resolution that jumps out to me the most is, "Enhance how we tell internal audit's story." I don't think it's the most important one on the list necessarily; however, anyone at any level in an internal audit department can contribute to being more proactive and intentional about sharing stories of internal audit adding value.

**FRANK HOLLOWAN** comments on the Chambers on the Profession blog post, "Five Internal Audit Resolutions for 2020 and Beyond" (InternalAuditor.org).

## Keep It Simple

Why make it complicated for nonaudit professionals when you can make it easier? The audit report is the easiest thing a diligent professional can explain to the most uninformed on this matter, in an understandable language. Everybody can understand what "confidence" means and what "protection" means. Albert Einstein once said, "If you can't explain it easily, you don't understand it well enough."

**SÉDUISANT TAZ-MBODI** comments on the Points of View by Pelletier blog post, "The Key to Better Internal Audit Reports" (InternalAuditor.org) on Facebook.

## Targeting Government

Weak controls, outdated infrastructure, and easily tricked employees make governments—especially state and local—ripe for data breaches and ransomware. It's a tough situation to solve with limited budgets and politics involved.

**HAL GARYN** comments on Tim McCollum's "Governments Under Cyber Siege" (InternalAuditor.org) on LinkedIn.

## Why We're in the Profession

I could not agree more with Norman's assertion, that integrity must take precedence over our job and our career. In my 10-plus years as an internal audit professional, I never thought the day would come when I would actually experience something like one of his examples. However, I found myself in a situation with the inevitable outcome of either my resignation or dismissal. I was terminated on Dec. 13, 12 days before Christmas. If it weren't for my experience, I would never have realized how many other internal audit professionals have had

**Ia**  
INTERNAL  
AUDITOR

FEBRUARY 2020  
VOLUME LXXVII:1

**EDITOR IN CHIEF**  
Anne Millage

**MANAGING EDITOR**  
David Salierno

**ASSOCIATE MANAGING EDITOR**  
Tim McCollum

**SENIOR EDITOR**  
Shannon Steffee

**ART DIRECTION**  
Yacinski Design

**PRODUCTION MANAGER**  
Gretchen Gorfine

### CONTRIBUTING EDITORS

Wade Cassels, CIA, CCSA, CRMA, CFE  
J. Michael Jacka, CIA, CFCU, CFE, CPA  
Steve Mar, CFA, CISA  
Bryant Richards, CIA, CRMA  
James Roth, PHD, CIA, CCSA, CRMA  
Rick Wright, CIA

### EDITORIAL ADVISORY BOARD

Jennifer Bernard Allen, CIA  
Dennis Applegate, CIA, CPA, CMA, CFE  
Lal Balkaran, CIA, FCPA, FCGA, FCMA  
Andrew Bowman, CPA, CFE, CISA  
Robin Altia Brown  
Adil Buhariwalla, CIA, CRMA, CFE, FCA  
Wade Cassels, CIA, CCSA, CRMA, CFE  
Stefanie Chambers, CIA, CPA  
Faizal Chaudhury, CPA, CGMA  
James Fox, CIA, CFE  
Nancy Haig, CIA, CFE, CCSA, CRMA  
Sonja Heath, CIA  
Kyle Hebert, CIA  
Daniel Helming, CIA, CPA  
Karin L. Hill, CIA, CGAP, CRMA

J. Michael Jacka, CIA, CFCU, CFE, CPA  
Sandra Kasahara, CIA, CPA  
Michael Levy, CIA, CRMA, CISA, CISSP  
Merek Lipson, CIA  
Michael Marinaccio, CIA  
Alyssa G. Martin, CPA  
Joe Martins, CIA, CRMA  
Stephen Minder, CIA

Rick Neisser, CIA, CISA, CLU, CFCU  
Hans Nieuwlands, CIA, RA, CCSA, CGAP  
Manish Pathak, CA  
Bryant Richards, CIA, CRMA  
James Roth, PHD, CIA, CCSA  
Jerry Strawser, PHD, CPA  
Glenn Summers, PHD, CIA, CPA, CRMA  
Robert Taft, CIA, CCSA, CRMA  
Brandon Tanous, CIA, CGAP, CRMA  
Stephen Tiley, CIA  
Robert Venczel, CIA, CRMA, CISA  
David Weiss, CIA  
Rick Wright, CIA

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

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

### CONTACT INFORMATION

**ADVERTISING**  
[sales@theiaa.org](mailto:sales@theiaa.org)  
+1-407-937-1388; fax +1-407-937-1101

**SUBSCRIPTIONS, CHANGE OF ADDRESS, MISSING ISSUES**  
[customerrelations@theiaa.org](mailto:customerrelations@theiaa.org)  
+1-407-937-1111; fax +1-407-937-1101

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

**PERMISSIONS AND REPRINTS**  
[editor@theiaa.org](mailto:editor@theiaa.org)  
+1-407-937-1232; fax +1-407-937-1101

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

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



PUBLISHED BY THE  
INSTITUTE OF INTERNAL  
AUDITORS INC.



New Thought Leadership from TeamMate

# Talent Elasticity: Rethinking the Workforce

Four of Five CAE's struggle to attract and source talent in their teams. The skills gap and scope of work is growing. The pace of change in organizations is staggering. The traditional approach to attracting and sourcing talent is not viable as a long term solution. This GAM session discusses current viewpoints from a recent study conducted by Wolters Kluwer TeamMate on possible options to source talent in a completely new way.

**Sign up for the Session at GAM 2020:**  
"Talent Elasticity: Rethinking Audit Resourcing"  
Tuesday, March 17, at 2:00pm

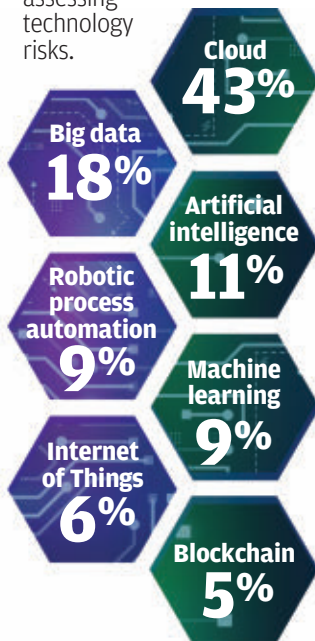
**View our Recorded Webinar on Talent Elasticity in Internal Audit:**  
[www.TeamMateSolutions.com/Talent](http://www.TeamMateSolutions.com/Talent)

COSO guidance addresses cyber risk... Deploying AI proves challenging... Internal audit's data governance role... Boards prioritize data and disruption.

# Update

## BEHIND THE CURVE

Few risk managers are fully capable of assessing technology risks.



Source: Accenture, 2019 Global Risk Management Study



## 2020 RISK PERSPECTIVES

Culture and talent are top concerns for business leaders this year.

Boards and senior executives around the world are most concerned about uncertain economic conditions and future regulatory changes. Yet, almost half of the top risks that worry them are related to culture and talent, according to Executive Perspectives on Top Risks 2020. The report was published by North Carolina State University's Enterprise Risk Management Initiative and Protiviti Inc.

Businesses will need to retrain their employees, "particularly as digital innovations, such as artificial intelligence (AI), natural language processing, and robotics, become a mainstay in organizations," says

Jim DeLoach, a Protiviti managing director and co-author of the report.

More than 1,000 board members and executives rated 30 macroeconomic, strategic, and operational concerns. The top five were:

1. The impact of regulatory changes.
2. Economic conditions that may restrict growth opportunities.
3. Succession challenges, and attracting and retaining top talent.
4. Inability to compete with "born digital" competitors because of the limited resilience of legacy IT infrastructure.
5. Limited organizational agility because of resistance to change.

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

IMAGES: TOP, SYLVERARTS / ISTOCK.COM; LEFT, ARTHHEAD / SHUTTERSTOCK.COM



The report includes diagnostic questions boards and executives can use to examine how their organizations approach risk management and oversight in the digital age as well as identify areas requiring significant improvement. It advises them to address the impact of leadership and culture on the risk management process and ensure there is a

sufficiently robust risk management process in place. Leaders should determine whether the risk focus is sufficiently comprehensive and clarify who is accountable for managing risk. Moreover, they should communicate an enterprise view of top risks and board risk oversight, the report recommends.

—S. STEFFEE

## THROUGH A CYBER LENS

Guidance applies ERM framework to cyber risk.

**A** stronger board focus on cybersecurity means adding experts in managing those risks, says guidance from The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Authored by Deloitte, *Managing Cyber Risk in a Digital Age* applies COSO's *Enterprise Risk Management—Integrating With Strategy and Performance* framework to cyber risk.

COSO Chairman Paul Sobel notes that boards and senior executives must set a strong tone at the top about cyber risk and “challenge the status quo of their ERM programs.” He says, “A business-as-usual approach to cyber risk management is bound to result in catastrophic damage.”

Not only are threats rising, but regulators are requiring boards and senior



management to address them, says report co-author Mary Galligan, managing director in cyber risk services at Deloitte & Touche LLP.

The report recommends organizations set up a team of senior executives to assess and manage enterprisewide cyber risks based on the ERM framework. By viewing these risks through the framework's lens, Galligan says leaders can “make strategic decisions with cyber risk always in mind.” —T. MCCOLLUM



**MORE THAN  
75%**

of respondents say risks from extreme heat waves and destruction of natural ecosystems will increase this year.

**NEARLY  
90%**

of respondents born after 1980 say these environmental threats will be aggravated this year — ranking them as their top 2 risks.

“It’s critical that companies and policy-makers move faster to transition to a low carbon economy and more sustainable business models,” says Peter Giger, group chief risk officer, Zurich Insurance Group.

Source: World Economic Forum, Global Risks Report 2020

## AI DEPLOYMENTS MORE DIFFICULT THAN EXPECTED

Companies find implementation is a tough challenge.

**B**usiness leaders seem to be undergoing a reality check when it comes to artificial

intelligence (AI). Only 4% of executives surveyed for PwC's 2020 AI Predictions report plan to deploy AI enterprisewide this year. In a similar poll the firm conducted last year, nearly five times as many said they

planned to deploy AI at scale in 2019.

Despite the decline in rollout expectations, 90% of the more than 1,000 U.S. business and technology executives surveyed say the technology offers more



# FAILURE

*to make the grade*

## AMERICAN CORPORATE GOVERNANCE INDEX

The new American Corporate Governance Index (ACGI) is a collaboration of The IIA and the University of Tennessee Neel Corporate Governance Center. ACGI uncovers shortcomings in governance practices among publicly held companies, with insight into where improvements must be made. **Know the score for American corporate governance.**



**Download your free copy today.**  
[www.theiia.org/ACGI](http://www.theiia.org/ACGI)

benefits than risks. Moreover, 18% say their organization has already implemented AI in multiple areas, 13% plan to do so, 42% are investigating its use, and 23% have conducted pilots within discrete areas. Nearly half expect AI to disrupt their geographical markets, the sectors in which they operate, or both.

The main reason for executives' retrenchment compared to last year, PwC says, is that companies have realized they need to tackle the fundamentals of AI before getting fully up to speed. With that in mind, the firm lists priorities for companies to consider to benefit from AI technology in the years ahead. For example, the report advises organizations to concentrate AI efforts on back-office tasks and automation to obtain return on investment and lay the foundation for long-term transformation.

PwC also recommends that organizations focus more on AI risk, noting that only about one-third of respondents say they have fully tackled risks related to data, AI models, outputs, and reporting. The report cites bias in algorithms and deep-fakes—fake audio or video created with AI—among risk-related issues to address. Other areas to consider include AI training strategy, integration with other technologies, and business model adoption that integrates AI's cognitive assets and processes.

—D. SALIERNO

## DATA RISKS RUN DEEP

Internal audit can serve as a partner to data governance, says Kevin Mooney, senior director, Enterprise Data Governance, Cleveland Clinic.



### What are the data governance risks and how can internal auditors help address them?

Failing to govern exponentially increasing volumes of data may result in risks that are dozens deep. These may include not knowing what or where your data is; perceived lack of trust in data; gathering and keeping low value/no value data; and lack of enterprise standards, teamwork, and accountability. Additional risks are inconsistent data-sharing practices, inconsistent or low-return commercialization, lack of understanding of the data's context, disconnected databases, redundancy, and proliferation issues. Security, cyber, and regulatory risks also are concerns,

along with integrity and quality issues. Lastly, lack of trust by both consumers and within the organization may result in a breakdown of using data for intended and compliant purposes.

There is value in data governance partnering with internal audit, but audit needs to retain its independent and objective status in that partnership. To avoid conflicts of interest, this could mean one internal audit resource contributes risk feedback to data governance initiatives. Meanwhile, another resource works independently to schedule audits on that data governance function and provide feedback to the board related to adequate risk mitigation. This, in turn, can help provide direction or strategy to the data governance function.

## PRIORITIES FOR A DISRUPTIVE YEAR

Report says data and disruption should top board agenda.

Linking boardroom discussions on strategy, risk, and global disruption and approaching cybersecurity and data privacy holistically are key topics for boards to consider in 2020, says a report from KPMG's Board Leadership Center (BLC). Addressing these challenges, the BLC notes, demands a combination of "near-term focus, agility, and long-term thinking."

The center's On the 2020 Board Agenda report cites trade wars, Brexit, rising populism, and potential military conflict among expected sources of global disruption. Moreover, business models may be disrupted by technologies such as robotic process automation, artificial intelligence, and blockchain. The BLC recommends boards reevaluate how they assess disruption-related risks.



Regarding data, the center suggests combining data integrity, protection, and availability under the umbrella of data governance. It advises making sure a robust framework is in place to govern data collection, storage, use, and decision-making. The BLC recommends examining responsibility for data governance across the business.

—D. SALIERNO



# Back to Basics

BY JACK PELIKAN    EDITED BY JAMES ROTH + WADE CASSELS

## SPECIALIST OR GENERALIST?

As today's internal auditors are being called on to do more, they face decisions about the focus of their careers.

The saying, "a jack of all trades is a master of none, but oftentimes better than a master of one," provokes debate between specialists and generalists. This discussion extends to many fields, including internal auditing.

As internal audit's role continues to grow, today's practitioners are asked to do far more than their traditional responsibilities around operational assurance and regulatory compliance. This paradigm shift is particularly evident in The IIA's Pulse of Internal Audit survey. The inaugural 2011 report lists fraud investigations, financial reporting, controls, compliance, and ethics investigations as the top areas of responsibility outside of traditional roles. In contrast, the 2019 report illustrates internal audit's growing involvement in other key areas including cybersecurity, enterprise risk management, cost/expense reduction, and third-party risk.

Internal auditors are not only expected to broaden their scope of services, but also deepen them. Most audit functions believe they are falling short technically in key areas, as evidenced by lower competency ratings (scale of 1–5 with 5 as highly competent) in cybersecurity and IT audit (2.9), data analytics (2.9), and technical accounting standards (2.5–2.9) in Protiviti's 2019 Internal Audit Capabilities and Needs Survey.

These seemingly conflicting qualities of depth and breadth raise an important question frequently asked by chief audit executives (CAEs) and practitioners alike: Is it better to specialize or generalize?

### The Practitioner

First and foremost, the practitioner's interests and career goals should guide any decision on specialization. On one hand, experienced practitioners may

become specialists over time, whether intentionally through career planning, mentorship, technical training, and workload, or unintentionally through trial, error, and, ultimately, success within certain disciplines. Alternatively, audit new hires may find generalization appealing as it provides a means to learn various aspects of the business and explore alternate career options, or identify opportunities for future specialization within internal audit.

While audit new hires may be more likely to start their careers as generalists, audit leaders should not deter them from exploring specialization. As academic institutions and continuing professional education providers expand their offerings in highly technical areas such as cybersecurity and data analytics, new hires can enter the audit workforce with skills best suited for specialist roles.

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 [jack.pelikan@theiia.org](mailto:jack.pelikan@theiia.org)

Regardless of experience level, practitioners may already have expressed specific interests or disinterests that will help department leadership better align projects with the appropriate resources. For instance, a new audit staff member may not have a specialization, but wants to limit his or her workload to IT audit and consulting projects. While smaller audit functions may not have the headcount or budget to allow for specialists, audit leadership must continuously engage their staff, understand their career aspirations, and foster their interests through mentorship and continuing education. If leadership does not facilitate these conversations, auditors should initiate the dialogue and ensure they receive opportunities to pursue their career interests.

### The Department

Every internal audit team is unique with respect to size, role, collective experience, and expertise. Therefore, a prescriptive ratio of specialists to generalists does not exist. Nonetheless, CAEs and auditors should have a clear understanding of their department's mission, and the current risks and needs of the stakeholders they support. For example, an audit department of four at a mid-sized private company with relatively low compliance risk may emphasize versatility, and operate as

**Every CAE will have a different vision for the department's workload.**

interchangeable parts to support one another and respond to the dynamic needs of its stakeholders.

Alternatively, a large international corporation with an audit staff of 50 may have more defined and consistent roles for its team members, including designated subject-matter experts based on country, business unit, or discipline.

### The CAE

Whether the emphasis is on agility, expertise, or some combination, every CAE will have a different vision for the depth and breadth of the department's workload. Because this vision can be shaped by the goals, interests, and skills of the staff, needs of the organization, and size and role of the function, CAEs should benchmark these items against the long-term goals of the department. For instance, if the department has established itself as a trusted compliance watchdog, but the CAE has longer-term ambitions of growing its advisory wing, the CAE should establish a formal strategy that encompasses recruiting, training, project mix, and stakeholder engagement to ensure these goals are achieved.

Furthermore, an opportunistic CAE with the optimal combination of resources and corresponding organizational needs may counter the specialist/generalist question by asking, why not both? While it seems contradictory to be a specialist and a generalist, CAEs can recruit and develop a diverse staff that includes both to ensure expertise and flexibility to respond to dynamic organizational needs.

### The Organization

As a shared service, internal audit has an obligation to provide value to its varied internal stakeholders. Often, an organization's copious needs may not be fully met by internal audit's finite resources. As a result, audit departments should use enterprise risk assessments, materiality, and stakeholder feedback to identify the most pressing organizational needs and impactful project opportunities.

Additionally, organizations without dedicated departments or subject-matter experts in disciplines such as enterprise risk management, data analytics, and cybersecurity may be more inclined to seek out internal audit to help address needs in these areas. This is provided that the audit team has specialists with the requisite expertise and availability. For instance, a large company with a robust data analytics

department may be less likely to engage internal audit to perform similar work than a smaller organization without a dedicated analytics function. Nonetheless, internal auditors can still provide value under those circumstances by assisting the analytics department with

tasks such as validation of the completeness and accuracy of the data sets used and providing context to analytical results based on their knowledge of the business.

### Align Talent With Needs

Internal audit's expanded role has afforded today's CAEs and practitioners new opportunities with respect to the depth and breadth of their workload, but it also presents new challenges and decisions around the merits of specialization versus generalization. These decisions should not be made in a vacuum, but rather through careful and informed considerations, including practitioner goals and interests, audit department size, role and vision, and organizational needs. But regardless of whether one is a "jack of all trades," a "master of one," or a hybrid of the two, internal auditors can maximize their value by aligning their talents and workload with their stakeholders' needs.

**JACK PELIKAN, CPA, CISA, CISSP**, is a senior director of internal audit at Caleres Inc. in St. Louis.

## AUDITING THE BOTS

To realize the benefits of robotic process automation, internal audit needs to help the business address the risks.

Imagine an internal auditor who is confronted with a disastrous robotic process automation (RPA) implementation. Her company spent millions of dollars to implement 50 robots, or “bots,” but the project had yielded only a single functioning bot. Making matters worse, hackers compromised that bot and drained the company’s bank account with a succession of undetected \$0.99 electronic transactions. Could the auditor have prevented these things from happening?

RPA can potentially reduce costs, improve accuracy and productivity, and eliminate tedious processes. It works by building software robots that can mimic the actions of a person on a computer, automating otherwise manual processes.

Bots are highly fragile and are not intelligent. Unlike artificial intelligence, they can only do exactly what they are told to do. And access to the technology

is growing, with Microsoft recently adding RPA functionality to Microsoft Office, putting it on millions of corporate desktops.

As with any new technology, internal auditors must be aware of RPA’s risks. The potential for a bot to make a mistake multiple times in seconds creates unique risks to assess.

### Validate Security Risks

Assessing RPA’s risks must begin with considering access security to the bot. RPA providers offer both on-premises and cloud-based solutions, with all the risks typical of these approaches.

Most RPA solutions do not house any “at rest” data, reducing the risk that sensitive data will be captured if the bot is hacked. Instead, bots operate on an organization’s applications using credentials just as a human user would. That means a bot can be hacked and coded to perform fraudulent, unethical, or hostile actions.

Examining the security around the RPA tool is critical, including access restrictions. Auditors should understand the security around each of the applications that the bot accesses and the controls around data that the bot “writes.”

As internal auditors begin to operate within bot-enabled environments, they should consider whether the bots are achieving their business purposes. Internal audit should be a partner, along with information security, in all RPA implementations. Their independent advice should improve clarity around the business objectives for each bot development. Business analysts should establish and track clear, objective performance metrics. Auditors should provide assurance about whether the bots are fulfilling their missions and meeting compliance objectives.

An additional challenge is disagreement about segregation of duties issues

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 [chris.denver@theiia.org](mailto:chris.denver@theiia.org)

around bots. Because bots lack a sense of doing “wrong,” some auditors say programming them with incompatible duties does not violate segregation of duties. Others say such programming introduces additional fraud risk because a person will have access to the bot’s program while in the production environment. Each organization should address this issue within its risk management framework and culture.

### **Audit the Development Life Cycle**

Internal audit should provide assurance of the organization’s RPA developments. Development of each bot should follow the organization’s system development life cycle (SDLC).

**System Changes** Auditors should consider both the “upstream” systems that the bot pulls data from as well as the “downstream” systems that the bot writes data to. That is because bots break easily in dynamic environments, requiring constant reprogramming and sometimes complete redevelopment. Any change in a relevant system can create an irreconcilable error in the bot’s performance. Auditors should ensure that the SDLC considers these issues.

**Bot Access** A best practice is to have one person create and test the bot in a “sandbox” —a controlled space outside the production environment. From there, another person moves the bot into production, while a third person manages its ongoing activities.

**Governance** Internal audit should be concerned with both ownership and governance of all active bots, looking for potential conflicts within the governance structure. Some organizations house the RPA program within IT, others at the business-unit level, and still others within a shared services area. Additionally, many organizations manage bot governance through centers of excellence that develop and manage the overall RPA strategy.

**Bot Activity** Most RPA solutions offer audit logs to facilitate review of the transactions each user conducts during a logon session. Auditors should examine RPA user profiles to identify segregation of duties conflicts, excessive access levels, access provisioned to terminated employees, and activity conducted by terminated bots. Additional reviews of the audit

## *Make Your Team Rock Solid*

**Train your team** by bundling any combination of in-person and online options with IIA Group Training. We’ll even bring IIA Training to your location. No matter what your team development needs, The IIA will tailor our training to meet your goals.

*Our place or your place. Our pace or your pace.*

Get a **FREE** group training consultation by calling  
+1-407-937-1388 or email [TeamDevelopment@theiia.org](mailto:TeamDevelopment@theiia.org).



2019-2305

---

# 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](https://www.InternalAuditor.org).

**Ia**  
INTERNAL AUDITOR



logs can reveal inappropriate activities, including attempts to repurpose the bots while in production.

A common practice is to provide each bot with a set of system credentials to access the enterprise resource planning system. In reviewing audit logs for the organization's non-RPA systems, auditors should look for irregular bot activities, as well as interactions with human credentials that might create a segregation-of-duties issue. Poor governance over RPA can allow a single person to use a bot to commit fraud.

### Managing Organizational Change


In the story about the internal auditor faced with a poor RPA rollout, the culprit was the company's culture. Employees had been reading articles about bots taking their jobs and fought the success of the implementation. What the company did not do well was communicate the RPA program's objectives and achieve cultural buy-in.

A consistent theme of successful RPA implementations is beginning by automating a single, high-impact, high-visibility process. A great candidate is a highly manual, tedious process that one or more employees dread doing. Once this process is

automated, it frees employees from a mundane task, enabling them to add greater value to the organization.

A further consideration for internal audit is assessing the capabilities and competencies of the internal and external personnel tasked with developing and managing the company's RPA program. Have each of these people been trained in RPA? Are roles adequately segregated, documented, and understood? Auditors should review the credentialed training programs offered by RPA vendors and seek training, themselves.

### Improving the Odds

Internal auditors should be frequent advisors throughout RPA initiatives. To be effective, the audit function must establish an appropriate baseline of controls around bots and include RPA in its audit plan. Moreover, auditors can provide independent advice on prioritizing the best automation opportunities. In this way, internal audit can improve cultural acceptance and improve the odds that RPA will benefit the business. 

**CHRIS DENVER, CPA**, is a Chicago-based national practice director with International Financial Group Advisory.

## Accelerate Your Success

Demonstrate your organizational, ethical, and internal audit leadership skills by obtaining the Qualification in Internal Audit Leadership® (QIAL®), the premier designation for internal audit executives, and prove to stakeholders you have what it takes to lead.

Drive in the lead position. [Learn more.](http://www.theiia.org/QIAL)  
[www.theiia.org/QIAL](http://www.theiia.org/QIAL)

 The Institute of  
Internal Auditors

# Risk Watch

BY SARAH DUCKWITZ    EDITED BY RICK WRIGHT

## RISK IN SESSION

CAEs and audit committees can use executive sessions to enhance the organization's risk culture.

**E**xecutive sessions should be on the agenda of every audit committee meeting. This means that all members of management leave the room, and the chief audit executive (CAE) has time alone with audit committee members. Executive sessions enable the committee to share risk concerns candidly. Scheduling an executive session at every meeting makes it less unusual when the CAE needs to ask for a session to discuss a specific concern.

While audit committee agendas can be routine and well-defined, executive session agendas normally are less clear. Although the CAE may have a few prepared remarks, these sessions typically revolve around one question asked by the audit committee: "Is there anything we need to talk about this time?" Yet, CAEs can make these executive sessions more valuable by engaging committee members in a dialogue about the organization's risk culture.

### Set the Agenda

As with the full audit committee meeting, having an agenda for the executive session is helpful. This should be a casual agenda that is not distributed; instead, the CAE should use it to ensure the session covers all topics of interest. The executive session agenda can include standard updates and risk topics specific to committee member concerns.

Because committee members may not know what to ask CAEs during executive sessions, CAEs can engage the audit committee in a variety of topics, including risk culture — how the business understands and manages risk.

In preparing for executive sessions, CAEs can create a list of ongoing and meeting-specific topics that address risk culture. Examples include tone at the top, corporate culture, governance, or overall risk monitoring. CAEs can provide insight into these areas without the

committee having to ask for it, while hearing committee members' perspectives.

### Share Risk Perspectives

Communication in executive sessions is a two-way street. The committee can provide valuable information to the CAE, while the CAE can share risk information and preferred action steps. During the session, the CAE can ask:

- ➔ What decisions is the board contemplating that may represent a strategy change?
- ➔ What concerns do audit committee members have about specific strategies or risks?
- ➔ What risks should internal audit prioritize?

Additionally, listening to committee member concerns is valuable for understanding what they view as important.

For CAEs, targeted questions can yield details that may lead them to update the audit plan or add a project to ensure risk

SEND RISK WATCH ARTICLE IDEAS to Rick Wright at [rick.wright@yrcw.com](mailto:rick.wright@yrcw.com)



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

coverage is timely and relevant. For the committee, discussing a specific concern or question can prompt the CAE to share white papers or training information in the materials for future meetings. The better the committee understands risk and its true impact, the better it can influence the risk culture with the board and management.

### Request Focus or Action

Because some topics can be politically charged, executive sessions exclude management to ensure open communication about sensitive topics. In the confidential environment of the session, CAEs can discuss risks that are not receiving necessary management focus along with recommended actions. For example, a change in privacy laws may require specific action by the organization. If the organization is not acting swiftly enough to comply, the CAE can alert the committee.

CAEs should share the specific requirements or a summary of the risk topic as background information for the committee, along with the potential impact and likelihood of occurrence. They should state whether the discussion is for the committee's awareness only or if they are asking for action.

These situations require tact. Unless the CAE is using the executive session to disclose fraud or wrongdoing by management, a no-surprises approach is best. In the privacy law example, the CAE should exhaust efforts to influence management to take appropriate action before bringing it up to the audit committee. As a courtesy, the CAE should inform management of plans to discuss the matter with the committee.

### Collaborate for Success


Sharing risk culture successes with the audit committee during executive sessions can help it better understand how internal audit impacts the organization's risk culture. For example, sharing ways that internal audit provided consulting or assurance services to a system implementation demonstrates the function's key role and proactive risk approach. Moreover, these examples can help committee members see future anomalies with how internal audit may be positioned or used. [la](#)

**SARAH DUCKWITZ, CPA**, is senior vice president and director of internal audit at Academy Bank and Armed Forces Bank in Kansas City, Mo.

**MONDAY**  
**MAR. 30, 2020**

**JOIN OVER 1,000**  
**INTERNAL AUDIT**  
**PROFESSIONALS!**

IAA Chicago Chapter 60th Annual Seminar  
— celebrating you our members!



The Institute of Internal Auditors  
**CHICAGO**  
*Cheers to 60 Years!*

**The Chicago Chapter is excited to celebrate its commemorative 60th Annual Seminar!**

Join the Chicago Chapter for a full day packed with presentations on transforming and evolving topics.


**JAN HARGRAVE** - The nation's leading Body Language Expert as seen on [New York Times](#), [NBC News](#), [ABC News](#), [CBS News](#), and [Fox Television](#), will teach how internal auditors should read and understand nonverbal communication to become more effective in *Body Talk*.


**TANMAY BAKSHI** - Artificial Intelligence Engineer, [IBM Champion](#), and [GOOGLE Developer Expert](#) will present on the Power and Value of Artificial Intelligence and display relevant transforming examples of this power.


**COLE NUSSBAUMER KNAFLIC** - Best-selling author and [CEO of Storytelling with Data](#) will show how raw data and data derived through analytics may be visualized and more importantly weaved into a compelling action-inspiring story.


---

25+ sessions including topics such as:

  
Data Analytics

  
Cybersecurity

  
Agile Internal Audit

  
Machine Learning

Visit [chapters.theiia.org/chicago/pages/default.aspx](http://chapters.theiia.org/chicago/pages/default.aspx) to learn more and register for this event. **We look forward to seeing you!**

# Fraud Findings

BY BRYANT RICHARDS

## THE FRAUD BEHIND THE FLAGS

A chief operating officer hid her multimillion-dollar scheme behind a cost-savings initiative.

After Greg Kane was promoted to director of internal audit at State Elder Care Co., a management firm for 54 long-term senior citizen care centers in Florida, his first objective was to refresh the risk assessment process. In his opinion, the previous director was too loose with his approach.

Kane met with department leaders as part of the risk assessment, including Tom Anderson, the director of purchasing. Purchasing was identified as an increasingly high-risk area because of the volume of spending and the absence of an internal audit in the last five years. According to Anderson, the department was deeply focused on a cost-savings initiative led by the chief operating officer, Dianna Foster. When asked how the initiative was going, Anderson eagerly expressed how 80% of spending from the 54 centers was consolidated to better leverage purchasing's

buying power and reduce expenses and costs.

Kane presented his risk assessment and internal audit plan to the audit committee, which included a review of the purchasing department. Foster resisted the inclusion of purchasing, insisting that the cost-savings initiative was not complete and that an audit would halt improvements. The audit committee agreed to the review primarily based on Kane's insistence that a high-risk area should not be ignored for more than five years.

Internal auditors started the review by testing purchasing controls and performing a high-level analysis of purchasing data, which included looking at overall spending trends by year. They also conducted walk-throughs of purchase order approvals, vendor master file additions, and the bid process. Satisfied with well-documented and performed controls, the auditors chose a sample of 30 purchased items and services

and tested them through all purchasing controls. Each test was perfect with three bids for each product, the best bid selected, approvals documented, and authorization levels followed.

When Kane met with his team, one auditor had an unusual comment about one of the samples—the 900 flags purchased the previous year for \$150 each for the centers. Having never considered the cost and durability of a flag before, the auditor thought this seemed like a large expense. A quick Google search found that reasonable, quality flags last approximately 90 days and cost around \$40. This resulted in a potential overspend of  $(\$150 - \$40) \times (900 - 200) = \$77,000$ .

Kane double-checked all the workpapers. Everything was in accordance with the purchasing policy, and controls appeared to be in place. And then it hit him. The audit team had not looked into the vendors. He Googled

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





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

## LESSONS LEARNED

- » Assume every unanswered question is important. In this case, the fraud would have gone undetected if not for the question about the flags. These unanswered questions do not always lead to fraud, but they will always add context to the state of the business and help demonstrate an understanding of the process reviewed by internal audit.
- » Analyzing data can be a powerful tool. However, it is always significantly more powerful when internal auditors know what questions to ask. Running ad hoc analytics midway through an internal audit is a great supplement to running a standard set of analytics at the start.
- » Adjust procedures based on risk. Plans are based on assumptions and should be adjusted once new information is discovered. The value of internal audit is not in meeting deadlines, but in helping to identify areas of improvement. As the risk of a process increases with new information, the potential value of audit procedures also increases.
- » High-risk areas should always be reviewed regularly. The possibility of a review each year would have prevented this fraud, as Foster would have been more fearful of getting caught. Each year after the first incident, the fraud nearly doubled in size. Catching the perpetrator in year three would have saved the company nearly \$10 million. Comparing this to the 300 hours of internal audit time and about 40 hours of purchasing employee time seems like a high return on investment.

the flag vendor but was unable to find a website. However, he learned that it was incorporated just two years before.

With this new insight, Kane and his team identified any items that increased in spending by 10% or more each year. Several items popped up, adding up to total expenditure of roughly \$200 million. The data showed that the items with increased spending nearly doubled each year. Within this sample, they identified items being provided by new vendors, which was nearly half of the sample.

The team then investigated each vendor within the bid process. Each bid appeared legitimate, but many of the companies providing the bids were recently formed and had no website. A few companies were consistently part of the bid process, whether they won or lost. When reviewing past bids, the team noticed that, in many cases, previous vendors were not included in the bid process. Kane's team documented its findings in preparation for a meeting with Anderson.


Kane explained that because of what he found with the flags, he decided to look at more data. Anderson turned pale. Kane asked how procurement chose the flag vendor and how often the flags need to be replaced. After a long silence, Anderson explained in a quivering voice how he and his team worked hard on cost savings and made great progress each year. Because he was short staffed, Foster helped administer bids for some of the items. It seemed like a great idea at first, but the number of items Foster managed grew each year.

Anderson admitted to rubber stamping many of the bids and approvals, assuming everything was above board. They were getting the same quality items they needed and cost savings were going up each year, so he did not think much

of it. But he became concerned two years earlier, after one of his long-term vendors contacted him about being excluded from the bid process. Anderson looked into the bid and was surprised to see that it came in higher than expected.

Kane and his team then looked into all the bids to identify the vendors. Twenty-one recently formed companies were new vendors to the company. Further investigation revealed that many of them were registered to Erin Foster, Dianna's sister. Kane and the vice president of legal went directly to the audit committee with their concerns.

For five years, Dianna Foster hid a \$15 million fraud behind the purchasing department's cost-savings initiative. She threatened to take business away from vendors if they did not agree to increase their costs by 20% to 30% and give her 80% of the increase as a kickback. One vendor, a hospice provider, agreed to pay Foster a personal referral fee for every senior referred from one of the elder care facilities. By year two, she realized that it would be easier to create companies and include them in the bidding process. The companies, run by her sister, would act as the pass-through for the business—buying the items from the prior vendor, marking up the prices, and splitting the money.

Dianna Foster was eventually arrested and sentenced to six years in jail and restitution. The organization of vendors Erin Foster created included 16 different companies and 87 unique bank accounts. Erin Foster was sentenced to three years in jail and restitution. 

**BRYANT RICHARDS, CIA, CRMA, CMA**, is an associate professor of accounting and finance at Nichols College in Dudley, Mass.

# A Voice in the Board

**M**

ost chief audit executives (CAEs) in North America report their findings to the organization's audit committee. The IIA recommends this practice, held globally to be part of the

gold standard enshrined in the three lines of defense model of corporate governance. Per the model's logic, CAEs sitting on the metaphorical third line have free reign to go anywhere and suggest organizational improvements, without fear of restriction or recrimination.

Getting to this position has been a fight for many CAEs, and some have still not achieved it. But The IIA's recent research, *OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*, has questioned whether reporting to the audit committee potentially constricts the value internal audit can add to some organizations. As businesses face a growing range of external threats, so internal audit's remit has expanded. Financial risk, once the mainstay of audit departments, today typically occupies only 20% of their time. Practitioners expend the rest of their effort on a diverse range of issues including cyber risk, disaster recovery, culture risk, climate change, and social responsibility, to name only a few.

This broadening of internal audit's remit raises the question of the extent to which a CAE should report to other board committees, and in what circumstances he or she should report to the full board. And, for those wishing to

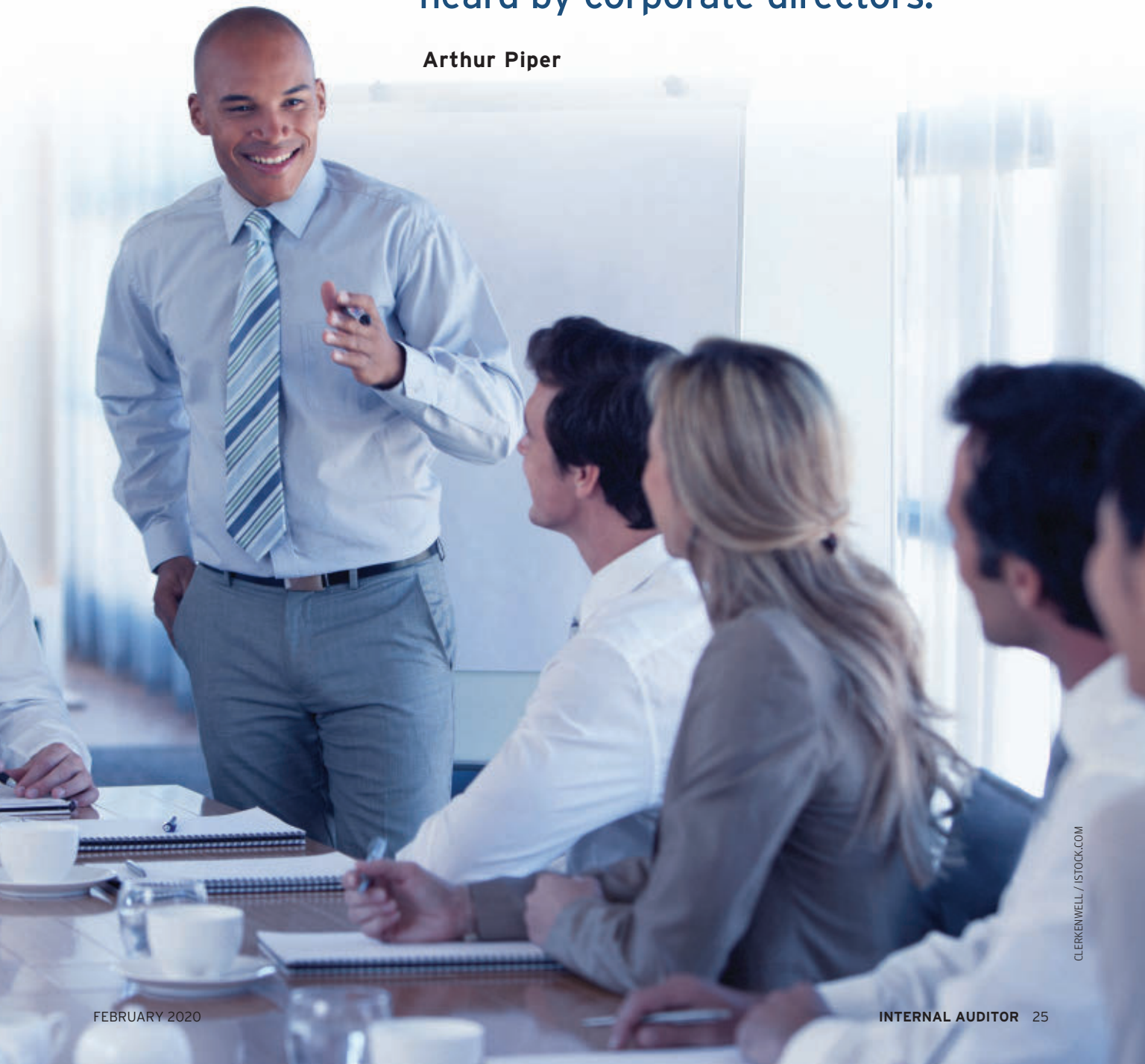


---

# room

Board members and audit executives weigh in on the best path to ensuring internal audit is heard by corporate directors.

Arthur Piper





explore that route, how can they get the audience and credibility to play this enhanced role?

### EXPANDING AUDIT INFLUENCE

Internal auditors are spreading their influence beyond the audit committee via other conduits to the full board, says Jenitha John, former CAE at First-

drawn together a whole range of corporate disciplines—from finance, audit, governance, compliance, risk management, and fraud to human resources and IT—because data is ubiquitous in organizations. “Internal audit has the ability to draw those teams together and collaborate with all of these other counterparts in the organization,” she says. “If you are not coordinating efforts on these matters, you are depriving internal audit teams from really growing and listening and serving the organization properly.”

To serve this more diverse constituency, internal audit needs to adopt the right approach and clearly communicate to the board the scope and focus of its work.

“Reshaping negative perceptions about internal audit is absolutely critical,” John says. “As a CAE you have to emphasize the fact that you’re pragmatic in your approach, you’re proactive, you’re collaborative, you’re agile, you focus on integrated risk-based auditing, you are educational, and that you can school your governing body and your management teams on controls, risk management, governance, and organization from a best process perspective. You don’t only focus on communicating audit observations, but you talk about business optimization and efficiencies by leveraging strengths across teams.” That can help open the door to the various board subcommittees and, on critical strategic issues, to the board itself.

### ESTABLISH CREDIBILITY

Living up to that ideal is not easy. Many CAEs lack credibility because they tend to emphasize box-ticking rather than focus on what matters to the audit committee, let alone the board, according to Dotty Hayes, a former CAE at both Intuit and Hewlett-Packard. Hayes is now chair of the board at First Tech Federal Credit Union in San Jose, Calif., and a board member and audit committee chair at

## Internal audit needs to clearly communicate the scope of its work.



“Reshaping negative perceptions about internal audit is absolutely critical.”

Jenitha John

Rand Bank in Sandton, South Africa, member of The IIA’s global board of directors, and former nonexecutive director on several boards. “The heartening aspect is that you see internal audit now not just serving the audit committee but also making submissions to other board committees,” she explains. John has seen internal audit increasingly called on to submit reports and present to risk committees, social and ethics committees, and even remuneration committees. “These meetings pertain to strategic issues that the company faces with regard to such topics as risk data aggregations, cybersecurity, information governance, the veracity of social matters (nonfinancial indicators), risk management, process maturity that influences bonus pool allocations, and so on,” she says.

Part of the reason for this trend has been the way businesses have approached tackling new guidance, such as sustainability reporting standards issued by the Global Reporting Initiative, and new regulation, such as the European Union’s General Data Protection Regulation (GDPR). “Regulation is causing various disciplines in organizations, which didn’t necessarily work together because they were operating in silos, to now actually converge,” John says. GDPR, for instance, has



# Nearly **half** of corporate directors say that at least one of their fellow **board members** should be replaced, according to PwC's 2019 Annual Corporate Directors Survey.

a range of organizations. CAEs must be able to bring matters to the board that are important to its members and demonstrate that the annual audit plan is risk-based and fits closely with the threats relating to corporate strategy. Informal meetings also can be a great place to build credibility, Hayes says. The audit team is invariably closer to the business than members of the audit committee, so it is best placed to detect trends across the organization or in isolated parts of the enterprise.

"It's probably not the full board, but the audit committee that is your primary interface as CAE," she says. "You know you have made it with them when they really care what you think: You're welcomed in as a strategic partner and, perhaps in a private session, you're asked your opinion on an issue that has to be handled very diplomatically—such as, do you believe what management has told us?"

Hayes says the credibility issue is even more important when reporting to the full board because space on its agenda for discussing a specific risk is scarce. But where a strong relationship exists, she suggests it could be valuable for the CAE to be invited to the top table. She says this may be appropriate when the internal audit team is reporting on the results of an investigation that has serious findings, for instance, or on topics of special strategic interest such as mergers and acquisitions. She also has seen this approach taken during an annual discussion of the risk appetite in an enterprise risk management program, a key strategic topic involving the full board. Most of the time, though, she sees the audit committee as the appropriate reporting channel for internal audit's recommendations.

But, she warns, the board has its own responsibilities in choosing the right CAE for the role. "The company has to hire an internal auditor who's got boardroom presence and can basically

go toe to toe with folks in explaining how the company and senior management needs to do something differently or better. If they haven't hired that kind of person, all hope is lost."

## **DEMONSTRATE VALUE**

Karen Brady, corporate vice president of audit and chief compliance officer at Baptist Health in South Florida, became chair of The IIA's North American Board early in 2018. Her theme for her year of tenure was "Find Your Voice," and she spent 12 months visiting hundreds of internal auditors across the U.S. and beyond to spread that message. She remains agnostic when it comes to the question of CAEs speaking to the full board, because she saw many different practices and arrangements that worked. In her own organization every member of the audit committee is also on the full board, so she says the reporting line to the audit committee is more than adequate.

But if internal audit wants to be credible with the board, or a board subcommittee, it has to be able to perform at the highest level. "Executive



**If you want to be perceived as valuable to the organization, you have to *be* valuable to the organization."**

Karen Brady

**To be credible with the board, internal audit must perform at the highest level.**

management tends to have conservative views of what internal audit can deliver, and that view follows through to the board because many executive officers also sit on audit committees in other organizations," she says. "CAEs need to be able to innovate and do things in ways that are above and beyond expectations to challenge those views. If you want to be perceived as valuable to the organization, you have to *be* valuable to the organization."

For Brady that means being perceived as a professional by sitting



Emerging technologies are a risk and an opportunity for internal auditors.”

Thomas Sanglier

for the Certified Internal Auditor exam and following the *International Standards for the Professional Practice of Internal Auditing*. Implementing Standard 1312: External Assessments, she says, is an important part of this. She is even more convinced now about the need for internal audit departments to have a quality assurance review of their function than before her tenure as chair. “Internal audit’s quality assurance review is objective assurance to the board that your department is effective,” she says. “It adds credibility, especially if on top of that you are prepared to innovate, to identify areas of improvement in the organization, and to focus on strategic risk areas.”

**UNDERSTAND EMERGING TECHNOLOGY**

Technology is a key area in which internal auditors can innovate—Brady is preparing for her team to learn robotics. She says almost all businesses are either currently considering or deploying a wide range of emerging technologies, from drones and robots to blockchain and artificial intelligence. It is a subject that Thomas Sanglier, senior director, internal audit, at Raytheon in Waltham, Mass., and author of the book *Auditing*

to your organization. If you are adding assurance to the board in such a critical area, on the other hand, you will gain credibility and may even have the opportunity to grow your team and scope of responsibility.”

One of the challenges for internal auditors is to choose the technologies most relevant to their particular industries, because trying to learn about several new technologies at once can be overwhelming, he says. Raytheon has set up internal working groups—called councils—for each new, relevant technology. Sanglier and his team have participated in those groups to understand how those technologies are being used in the company.

“If you know what is in your products and processes, you can ask the right questions about risk and risk mitigation,” he says. “If you are lucky to have a subject-matter expert in your business, hitch yourself to them and learn everything you possibly can.” But he warns of becoming overdependent on one person, a criticism leveled at CAEs who were seen to be too reliant on their chief information officers for assurance around IT in The IIA’s OnRisk 2020 research.

“People are looking at emerging technologies as being IT-led; that’s a mistake,” he says. Internal auditors need to be looking at how those technologies are going to operate in the business, and how they may affect products and services. More broadly, CAEs can help the board understand how well the organization is positioned to use emerging technologies. For example, Sanglier points out that many new technologies depend on acquiring and processing clean data from across the enterprise, but data governance is often poor. “If nothing else, internal auditors, as part of every single audit, can look at data governance for whatever emerging technology the business is considering. When the technology

One of internal audit’s challenges is to understand industry-relevant technology.

and *Disruptive Technologies*, has been focusing on for the past few years.

“Emerging technologies are a risk and an opportunity for internal auditors,” he says. “They are a risk because if you are unaware that robotic process automation is being used in your business, you are in the unfortunate position of missing an important risk

There is critical **misalignment** between how executives **view** an organization's capability to manage risks and what is communicated to boards, according to The IIA's OnRisk 2020 report.

comes—and it's coming—you're going to run into problems implementing it if the data is bad. It's an issue the board needs to know about."

### RESHAPING THE AUDIT COMMITTEE

While some may point the finger at internal audit for being too focused on detail, or for not exploring emerging threat areas, audit committees may also need to reform. In the U.K., for example, the financial services industry regulators require regulated firms to have an audit committee and a separate risk committee. The requirement has helped raise the profile of risk within those businesses. Plus, recent guidance produced by the Risk Coalition, an industry body that aims to establish consensus on risk management practice, recommends that the risk committee invite the CAE to its meetings "as necessary or appropriate."

Hanif Barma, one of the architects of the Risk Coalition and founder of the consultancy Board Alchemy, says many audit committees outside of the financial services sector would benefit from extending their remit to reflect the increased array of risks their organizations face. "Internal audit has changed from being largely focused on financial controls to becoming more concerned with the broader risk landscape," he says. "The question is, has the body it reports to changed sufficiently as well? In many cases, it has not. They are largely focused on financial control and financial reporting, rather than acting as audit and risk committees."

Reformulating the audit committee as a risk and audit committee could help internal audit develop a more strategic, risk-based role, he says. Barma chaired the board of a children's charity that has made such a transition. The change has helped the organization take a more holistic approach to

managing its risks, he says, and it has enabled the reformed committee to take deep dives into selected threats at its regular meetings. He explains that bringing those issues to a full board meeting may not be as effective

## Clearly, more CAEs are finding a voice beyond the audit committee.

because of the limited time they would receive. "To do internal audit justice, having a separate committee that gives focus to its work is really important," he says.

On the other hand, with issues of strategic importance, CAE presentations to the full board can be worthwhile. "What has been missing in the evolution of corporate governance is that internal audit has not had access to the full board," he says. "Perhaps the CAE does not have to sit through a full board meeting, but when the chair and company secretary are working on the board agenda, they should be considering whether there are issues on which the CAE could usefully come and give their perspective."

### EXTENDING INTERNAL AUDIT'S REACH

Clearly, more CAEs are finding a voice beyond the audit committee. As risk board subcommittees have emerged, auditors have been invited to contribute their expertise. Others have found a voice at other board subcommittees and, less frequently, in full board meetings. For those who have built up the credibility and clout, the opportunities to add value to their organizations have never been greater. [la](#)

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



“To do internal audit justice, having a separate committee that gives focus to its work is really important.”

Hanif Barma

# Automated Cross-Application Access Controls

The Fastpath Assure® suite is a cloud-based audit platform that can track, review, approve, and mitigate access risks across multiple systems from a single dashboard. A perfect fit for your 2020 strategy.



Segregation  
of Duties  
Analysis



Access  
Certifications



Audit Trail/  
Change  
Tracking



User  
Provisioning



Emergency  
Access

Stop by the Fastpath Booth #404 at GAM in March

Visit [gofastpath.com/ia](https://gofastpath.com/ia)



# *A Plan for Regulatory Change*

Nancy Haig

**N**

oncompliance with laws and regulations carries potentially steep consequences for organizations. Fines, penalties, sanctions, debarment, and public relations nightmares are among the many impacts of compliance failure, not to mention the reputational damage and loss of business that may occur. Moreover, failure to identify and consider laws and regulations may result in missed business opportunities and lack of strategic alignment. In many ways, neglecting to address and manage regulatory change can lead to significant organizational harm.

In fact, The IIA's recent OnRisk 2020 research identified regulatory change as one of the most critical risks facing organizations this year. Other risks included cybersecurity, data protection, business continuity, talent management, and third parties. Depending on the industry, each of the risks identified in the report may have a regulatory component. For example, organizations that fail to protect personal data through a cybersecurity control framework can face significant penalties. The data may have been processed through an insufficiently vetted third party, or by unqualified employees whose inclusion in the organization resulted from inadequate talent management. If a data breach occurs, the organization must be able to respond within regulatory time frames and,

**A top-down assessment model can help internal auditors keep tabs on regulations and ensure the organization is prepared for what lies ahead.**

depending on the significance of the breach, possess reliable crisis response and business continuity plans.

Internal auditors have a responsibility, under the *International Standards for the Professional Practice of Internal Auditing*, to help ensure their organizations are addressing and managing regulatory risk effectively. According to Standard 2120: Risk Management, internal audit “must evaluate the effectiveness and contribute to the improvement of risk management processes.” More specifically, according to The IIA’s interpretation for this standard, “The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding . . . compliance with laws, regulations, policies, procedures, and contracts.” Practitioners may benefit from an assessment tool aimed at achieving that objective.

### THE ASSESSMENT MODEL

Using a top-down framework based on compliance guidance from the U.S.

Federal Sentencing Guidelines, internal auditors can assess whether the organization is addressing and managing regulatory change effectively. Governments of other countries have emulated the guidance when outlining steps to ensure compliance with major laws and regulations. It can guide auditors, step by step, through a structured review of what’s to be expected by regulators in the management of regulatory risk.

### Identification of Laws and Regulations

The group responsible for identifying regulatory change can vary from one organization to the next. Depending on the size, regulatory complexity, and maturity of the organization, internal auditors may be able to perform a top-down assessment of how well the enterprise risk management program, or risk management function, identifies and manages changes in regulatory risk. Moving down a level, if these functions do not exist or are ineffective, auditors can

assess the overall compliance program, if one exists. Otherwise, the legal department may be responsible for identifying and disseminating information on changes in laws and regulations. And while not optimal, business management of each function, as the first line of defense, may hold sole responsibility for knowing and managing legal and regulatory changes, as well as regulatory risk overall.

To assess whether regulatory change is managed effectively, internal auditors should be aware of the common categories of laws and regulations that impact most organizations. These include employment/labor; tax; advertising; environment, health, and safety; financial crimes/anti-bribery/anti-money laundering/anti-trust; and data protection. Internal auditors must also be aware of the laws and regulations that impact their specific industry. Finding reliable sources of industry knowledge and perusing them regularly helps in the identification

## THE MODEL IN PRACTICE

To demonstrate how the model works in practice, consider the high-risk area of data protection – more specifically, the European Union’s General Data Protection Regulation (GDPR). The regulation’s purpose is to strengthen and unify data protection for individuals within the EU, regardless of where their personal data is processed. Non-compliance with GDPR carries steep penalties, with fines of up to 4% of worldwide turnover. Following the model’s cadence, internal audit can perform a step-by-step examination of GDPR-related change impacting the organization.

**Step 1.** After identifying relevant GDPR provisions, the organization performs a risk assessment to determine whether the regulation will impact it, and if so, how, where, and when. Because many organizations already have data protection controls in place, the assessment may include a gap analysis to determine changes or additions that may be needed to ensure compliance.

**Step 2.** Because data protection constitutes an area of high risk, and given the entitywide importance of data protection compliance, the organization establishes a compliance policy. Specific procedures are developed for the marketing function, as just one

example, to ensure all contacts are vetted before release of communications.

**Step 3.** The organization develops messaging and disseminates it to employees, explaining GDPR requirements, their impact on the organization, and each individual’s responsibility for compliance. The communication informs employees that the organization is developing GDPR policy and procedures, and provides a time frame for rollout of these items.

**Step 4.** The organization implements a training course for all employees that includes explanation of organizational policy on compliance with all data protection laws and regulations, and

# U.K. financial service providers cite regulation as their No. 1 concern over the next year, according to a recent survey conducted by technology firm Intelliflo Ltd.

process. And while the best sources will vary depending on country and industry, one free resource that compiles global legal analysis from law firms is Mondaq.com. Auditors may also find it helpful to develop relationships with those in the organization who would most benefit from sharing news of regulatory change.

**Risk Assessment** Regulatory change risk assessment occurs after identification of regulatory and legal requirements. Internal auditors should examine the effectiveness of processes in place to assess how and where regulatory change will impact the organization, and how that information is communicated to those who need to know. As with the identification process, which function performs the risk assessment depends on the size, maturity, and regulatory complexity of the organization.

**Policy Development** To help ensure all impacted employees—and in some

cases even third parties—understand what is expected of them, the organization needs to provide an overview of the new law or regulation. Regardless of which function develops such policies, the organization should have a standard template, centralized storage location, and established controls for publishing, reviewing, and updating them. Assessment of these elements may be included in the internal auditor's program.

**Compliance Procedures** Organizations develop procedures to provide employees with the exact steps they need to perform to ensure compliance with changes in laws or regulations. Procedures may be developed by a dedicated function, a committee, the chief risk officer, compliance, the first line of defense, or other areas. They may be published at the same time, and even within the same document, as the corresponding policy. Internal auditors may determine whether policies are



**TO COMMENT**  
on this article,  
**EMAIL the**  
**author at nancy.**  
**haig@theiia.org**

specifically on GDPR. During the training, employees are required to acknowledge the GDPR policy. Meanwhile, the marketing department employees, as one example, are trained on vetting contacts for campaigns.

**Step 5.** The organization has already established an anonymous reporting mechanism to help address any potential issues of noncompliance. However, it adds the data protection policy to both the hotline resources and the company intranet resource section.

**Step 6.** The organization implements monitoring controls. For example, emails sent directly by individuals to more than 40 external recipients

are reviewed each quarter for marketing content, to determine whether contact vetting controls may have been bypassed.

**Step 7.** Internal audit either reviews the second line of defense's program to ensure compliance with data protection regulations, or it reviews the specific elements that have been put in place, depending on the size, maturity, and regulatory complexity of the organization.

**Step 8.** If monitoring controls reveal that procedures are not followed, or if internal audit finds that elements of the program are deficient, the organization initiates corrective action.



IMAGES: THIS PAGE AND PAGE 34, BAKHTIAR ZEIN / SHUTTERSTOCK.COM

developed timely, are updated periodically, and describe the steps to be taken to ensure compliance.

**Regulatory Communication** The organization's communication on upcoming regulatory change may include general information about the change, implementation timing, and training. The targeted audience depends on who will need to comply. Communication may be in any form, including emails, intranet bulletins, and staff meetings. Regardless of the vehicle, communications about regulatory change should be maintained in a data repository as documentation for regulators, if needed. Internal audit may decide to assess the timeliness, effectiveness, and retention of the communication.

**Staff Training** Effective training is key to ensuring that employees, and in some cases third parties, understand the regulatory change and the importance of compliance. Depending on the targeted audience, training may be general or include specific procedures. For example, everyone in the organization needs to know the importance of complying with anti-bribery and corruption laws and regulations. However, employees in the finance department, for example, may need detailed training on how to monitor payments to ensure compliance.

Training should be provided to the appropriate targeted populations—including new hires and new third parties—as applicable. The training should include information on available resources, as well as specifics on how to report potential issues of noncompliance. Depending on the topic, targeted population, and in some instances regulatory requirements, the training may be provided online or in person. Regardless of the offering, detailed records of training completion must be maintained, and an escalation procedure should be in

place to follow up with individuals who have not completed the training.

### **Acknowledgment Procedure**

Employee and, in some instances, third-party acknowledgment of the regulatory change, and any corresponding policy and procedures, is critical to document and maintain. Acknowledgment often is tied to, or included in, training completion. An escalation process should be in place to ensure receipt, and documentation of follow-up efforts should also be maintained. Internal auditors can assess whether acknowledgments have been received and stored, and whether the escalation process has been followed.

**Whistleblower Hotline** An anonymous reporting mechanism, or whistleblower hotline, represents an important element of the overall legal and regulatory compliance program. Many organizations outsource this responsibility to third-party providers, which offer the ability to report online or by phone. The topics that may be reported depend on the data privacy regulations in each country, although most at least allow reporting of noncompliance with financial laws and regulations. In some countries, however, anonymous reporting is discouraged. The most effective reporting mechanisms include vetting of potential compliance concerns or questions.

The organization needs to have formal procedures in place for conducting investigations. The procedures should involve the functions that will lead or conduct the investigations, as well as legal counsel. They should also specify how the crisis management plan will be triggered, and the insurance carrier notified, as applicable, and a process for closing and reporting on each investigation. Internal audit may be part of the intake process and investigation. Regardless, internal audit may include in its review an assessment





# Three-fourths of retail executives expect **privacy** regulations to have a moderate to significant impact on their business, according to Deloitte's 2019 U.S. Consumer Data Privacy survey.

of how concerns or potential issues of noncompliance brought to the hotline are handled, closed, and reported.

**Monitoring Controls** The organization needs to implement monitoring controls to ensure that employees, and in some cases third parties, are following procedures. If procedures are not being followed, additional training may be warranted or disciplinary action may be taken, depending on the root cause. Often, the second line of defense establishes and performs the monitoring process. If that's the case, internal audit can review the work of the second line to assess effectiveness. Monitoring may be continuous or performed at periodic intervals. Regardless, the organization needs to follow established time frames.

**Compliance Auditing** Although often mistakenly combined with monitoring, auditing is a separate activity. Whereas the focus of monitoring controls is to ensure procedures are followed, auditing focuses on all of the elements that have been put in place to ensure compliance with regulatory change in a particular risk area. For example, a monitoring control to ensure compliance with insider trading laws may entail electronically scanning emails for keywords and phrases. Auditing for compliance with insider trading laws, on the other hand, would involve a review to ensure the establishment of policy, procedures, training, effective monitoring controls, and disciplinary action in the event of noncompliance. If the second line of defense is responsible for auditing the program's elements, internal audit may assess its effectiveness. Otherwise, internal audit would perform the audit, including a review of all of the elements.

**Corrective Action** The organization needs to take corrective action in response to monitoring, auditing, and

investigations. Corrective action may mean implementing additional or different controls or training, or disciplining noncompliant employees. In the case of discipline, employees should be treated equitably, regardless of their position in the organization. For example, a lower level employee should not be treated more harshly than a company officer for the same offense. Often, the organization assigns a committee to monitor equity of disciplinary measures across the board.

To ensure future compliance, control measures must be evaluated

## The right approach can help auditors get a bead on regulatory change.

whenever noncompliance is discovered. The review needs to be conducted timely and include root cause identification as well as implementation of appropriate controls.

### KEEPING PACE WITH CHANGE

Internal audit should serve as a trusted advisor to management by helping the organization address regulatory change. It all starts by understanding and staying current on industry-specific developments, and considering the regulations that may impact the organization. Using a top-down approach, internal audit may review the entire framework, the compliance program, or the specific elements in place, depending on its risk assessment. The right approach can enable internal auditors to get a bead on regulatory change and help ensure the organization is prepared for what lies ahead. [la](#)

**NANCY HAIG, CIA, CCSA, CRMA, CFSA**, is the director of internal audit and compliance for a global consulting firm in New York.



Russell A. Jackson

Audit leaders must make sure their teams have the right skills to serve their organizations effectively.

IMAGES: SKY, SUMROENG CHINNAPAN / SHUTTERSTOCK.COM; SKYDIVERS, MAURICIO GRAKI / ISTOCK.COM

# Forming Today's Internal Audit Function

**S**taffing an internal audit department capable of meeting the myriad and multiplying mandates imposed by a growing group of stakeholders is like solving a Rubik's Cube. The logistical difficulty of making multiple moving parts on more than one plane match up—at the same time—characterizes the way chief audit executives (CAEs) struggle to line up the right mix of talent with their organizations' evolving technical, analytical, and operational needs. But just as a Rubik's Cube can be solved, there is a solution for internal audit department staffing.

The solutions are unique to each situation, but alignment is key in all cases. "The internal audit function must first align its focus and staffing plans with the organization's broader goals and strategies," says Mike Maali, internal audit, compliance, and risk solutions leader at PwC LLP in Chicago, "then with the specific objectives of the internal audit department, itself."

But aligning staffing isn't simply a matter of hiring expert data analysts. Often, the work ahead requires core audit competencies, the basic capabilities every department is called upon to muster. So, audit leaders may need to add traditional, frontline practitioners to their rosters, too. And everybody in every position must be nimble and quick. Companies often change business models, and some of the new models lack regulatory conventions. Internal auditors must be able to

zoom in to see every point in detail, and zoom out to view the matter from a strategic angle.

## STAFFING THE RIGHT TALENT

The essence of the CAE's hiring challenge is determining the right mix of IT and business expertise, sharpened interpersonal skills, and audit fundamentals the department requires. "Finding the right people for an internal audit department is extremely hard," says Robert Berry, principal at consulting company That Audit Guy based in Mobile, Ala. Stakeholders, he adds, hear about the latest tools to use—blockchain, for example—and want internal audit guidance before they know with any clarity what they want from the technology. Do you staff to conduct research that's not going to be very relevant?

The evolution of the profession—and its professionals—can intensify the challenge. "It requires new internal auditors with different backgrounds to evaluate new operational and emerging risk areas," says Yulia Gurman, CAE at Packaging Corporation of America in Lake Forest, Ill. "Schools are producing more ambitious internal audit graduates, and the profession is attracting experienced candidates from other industries from a variety of backgrounds." The profession has evolved beyond evaluating compliance and reporting risks, she adds. A growing number of companies hiring internal auditors now emphasize emotional intelligence and professional skills as much as, if not more than, technical skills.

The CAE's task is to understand the organization's key risks, internal audit standards and requirements, and



stakeholder expectations, then assess whether the current staff has sufficient skills and expertise to provide the level of assurance required. “You also need to understand the complexity of the business and the size of internal audit teams at similar organizations,” says Stacey Schabel, American audit director at Jackson National Life Insurance Co. in Lansing, Mich., “because they directly link to your consideration of the levels, organization, and shape of your team.” She maintains an inventory of team members’ experience in audit and risk management and all critical focus areas, certifications supporting their expertise across focus areas, and professional backgrounds. “Mapping their skills and experience supports audit planning and detailed resourcing, including when to engage external expertise you don’t have on your team,” she says.

### AUDIT STAFFING DOS AND DON'TS

Competency catalogs like Schabel’s lay the groundwork for more strategic department staffing. Experts offer tips for ensuring internal audit departments have the people they need.

#### Make sure the basics are in place.

“A core set of internal audit skills must be addressed,” Berry stresses. Department staffers must know how to document work, draft reports, and communicate with clients. That’s always been the case for traditional businesses with established internal audit processes, but basic audit skills are even more important, Maali notes, for cutting-edge companies with untested business models and the firms those companies do business with. “Technical and analytic skills sets shouldn’t be overlooked, considering the complexity of some models,” he says. “Unknown things can happen when businesses are ahead of regulations, so foundational capabilities are really important.”

Schabel’s department also performs U.S. Sarbanes-Oxley Act of 2002 testing for the insurer’s Financial Reporting team. “While our risk-based plan focuses extensively on strategic risks and organizational innovation,” she says, “Sarbanes-Oxley testing is valuable as it is good training ground for new auditors and offers additional leadership opportunities for the team.”

**Don’t get stuck in yesterday’s definition of the basics.** What constitutes fundamental competencies changes over time, Maali says. “There is a redefinition of capabilities grounded in three dimensions: business acumen, analytics acumen, and technology acumen,” he says. “They form the baseline set of capabilities we expect all auditors to exhibit.”

Business acumen generally applies to basic internal audit areas of influence, including operational processes, compliance, and controls. Kamal Uddin Gazi Jishan, internal audit manager at Ali Bin Ali Holdings in Qatar, calls it “a crucial competency because business managers value the advice and services of an internal auditor who ‘speaks their language.’”

Technology acumen applies to the emerging tools being used—block-chain, artificial intelligence, Internet-of-Things—and, Maali notes, “internal audit needs capabilities relevant to their implementation or to ongoing monitoring and evaluation.”

Analytics acumen applies to staff members’ ability to master new audit techniques leveraging different sources of data. “Big data drives the need for a baseline of analytics capabilities,” Maali adds.

More advanced analytic skills may be mandated by stakeholders’ expanding corporate visions. “If it’s a broader set of risks beyond financial and compliance into operations and strategy,” Maali cautions, “you’re going to have a hard time meeting some of those expectations

if the team isn’t appropriately skilled.” That expertise may come from inside the company or outside hires, or consulting firms with internal audit capabilities.

**Tailor hiring practices to help achieve organizational goals.** “First, we need to know what is happening in our company, industry, peer groups, and the macroeconomic environment,” Gurman says. “Any changes or big strategic initiatives may require unique skills that our team members don’t currently possess.” That’s an ongoing evaluation, she emphasizes. In all areas, not just hiring, it’s key to making sure the internal audit department stays relevant to stakeholders’ needs and has the right tools to address risks and provide valuable insights to management and the audit committee.

Maali notes that, to date, existing internal audit competencies have typically been able to meet audit committee needs, and both sides generally have shared an understanding around them. While they’re often still grounded in their fundamental responsibilities, Maali says “boards are getting much more focused on emerging technology risks,” including cybersecurity and data protection concerns, especially operating in the cloud. Berry agrees that most changes to the profession are driven by changes in stakeholder expectations. “We see boards and management asking about technological processes, and everyone is concerned with personal data.”

In some cases, organizational objectives require specialized skills. Many companies, Maali points out, are undergoing digital transformations, for example. “Is your team equipped to operate in that environment?” he asks.

One company he cites is changing its business operating model and will be organized completely differently as a result. “That should cause internal audit to really examine how it’s organized,” he says. “Take your cue from



# Broader alignment with strategic priorities is a top focus area for internal audit departments, according to MIS Training's 2019 Internal Audit Priorities report.

what's happening with the business and make sure you're properly aligned."

## Sync hiring strategy to departmental objectives, keeping in mind the changing shape of internal audit's ambit.

Sometimes, the department's goals also may require specific skills. A department that relies heavily on data analysis to meet its goals, for example, will require specialists in data analytics. There are, Schabel notes, several facets to consider when determining what skills your team needs:

- » Business objectives and key risks to accomplishing them.
- » Organizational risk appetite and strategy.
- » Audit needs assessment requirements, such as ratings and cyclicalities.
- » Organizational and regulatory changes and focus areas.
- » Future vision—if it's digital advancement, for example, internal audit may need specific new expertise.

"Having a seat at the table so we are aware of the strategic vision and direction of the organization is key," she adds.

The paradigm hasn't changed completely, Maali says, but "in the last 12 to 18 months, there's been a shift toward migrating some of the Sarbanes-Oxley testing activity outside internal audit and into the controllership of the organization." Citing the three lines of defense refresh, he agrees with The IIA's focus on efficient testing and achieving the lowest total compliance cost that doesn't sacrifice effectiveness. "It points out the need for collaboration across the three lines," he says, "especially as the complexity of risk and the speed of business processes really rise."

## Build a team that can manage risks rather than adjusting your audit plan to match current staff's skills.

"Scope your audit plan to the risk,

then get the right capabilities to do it," Maali says. For example, an internal audit leader with little knowledge of cloud audits might work with a cloud audit expert to "get at the real risks and how to audit them." Where staffing gaps exist, he adds, companies usually build capabilities with existing people to the extent they can, then "supplement with strategic hires that accelerate the transformation of the skills."

Jishan's company's human resources policies generally encourage internal hiring, but transfers to internal audit are rare. "It's likely the opposite will occur," he says, "whereby an internal auditor is found to be the best fit candidate for a finance or management role."

But employees from other departments often have skills that can be fine-tuned to internal audit through professional education, thus enhancing their candidacy, Berry says. That includes courses in "at least two different industries," he adds—internal audit and the company's. "We have to be knowledgeable about audit standards and how to apply them on the job," he adds, "but also about the industry we operate in."

University curricula are being redefined, Maali says. "People are coming out of school now with a clearly different level of skills from just two or three years ago," he explains. "The aptitude level is higher, and that translates into people very ripe for learning new things."

Look for that to translate into passion for the profession, Jishan advises. "The sense of adding value to the business is the driving factor for a career-centric internal audit professional."

## Don't be limited by outdated impressions of the profession.

The profession moved away from primarily verifying financial statement and activities many years ago, Berry notes, leading to "different flavors of internal auditors." An engineering firm may hire a former engineer as an internal



We need to know what is happening in our company, industry, peer groups, and the macro-economic environment."

Yulia Gurman



Business managers value the advice and services of an internal auditor who 'speaks their language.'"

Kamal Uddin Gazi Jishan



Cutting-edge tools can't replace periodic contact with audit clients."

Robert Berry



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

auditor, he explains, or a hospital may hire a former nurse.

Gurman and her team now search in an expanded pool that includes professionals with engineering and psychology degrees, to name just two. She's also hired people with no internal audit experience, but a strong interest in joining the profession—adding their own valuable skills to the mix.

The deep expertise needed for specific projects can be found outside the organization, Maali says. "Balance specific needs with how much of the expertise is routinely needed," he adds. For areas you don't do much business in, only in an occasional audit, it might be worth it to lean on an external party for expertise. "Build it when it makes sense," he adds, "and buy it when you have a targeted use."

**PEOPLE SKILLS OUTWEIGH TECHNICAL SKILLS**


The challenges facing internal audit departments continue to expand as the profession's influence spreads throughout their organizations; but they can be managed with the growing diversity of talent available for hiring. Indeed, the human side of staffing—how the department functions when the team is complete—should be paramount, Schabel emphasizes. "The most effective, successful, and healthy teams have diverse backgrounds, knowledge and expertise, strengths and weaknesses, and ways of working," she says. That encourages individuals to hone their teamwork, conflict resolution, and interpersonal skills. So does getting out of the cubicle occasionally, Berry adds. "Cutting-edge tools can't replace periodic contact with audit clients."

Faced with two well-qualified candidates for one job opening, one of whom has an edge in technical skills, the other in people skills, Gurman says the hiring decision would be easy. "Technical skills most, if not everyone,

can learn if they really want to," she explains. "People skills are much harder to develop." Internal audit activities require all kinds of interaction with a variety of departments and people with very different personalities, she points out—and the interaction isn't always about delivering good news. Hiring decisions need to facilitate developing strong positive relationships with audit clients and colleagues throughout the organization. "Strong emotional intelligence and effective professional skills become even more critical, as internal auditors advance into department manager positions," Gurman adds.

**LINING IT UP**

Pressures on the profession continue to mount, as internal audit's role evolves into more strategic planning and operational consulting functions, and as practitioner preference pivots to positions that involve closer contact with colleagues, managers, and C-suite executives. At the same time, advances in technology demand both highly developed analytical skills and command of basic internal audit functions. For CAEs with jobs to fill, "Hire some numbers pros" has been replaced with "Staff to the company's strategic goals."

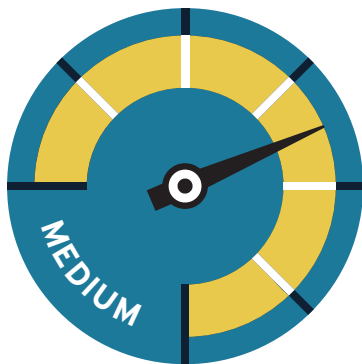
Diverse candidates for the increasingly diverse positions CAEs offer makes that mandate easier to accommodate. Professionals from a variety of fields are drawn to internal audit—some looking for old school "box checking" jobs, others with their eyes on "trusted advisor" responsibilities—and, more often, they're already skilled at both analytics and politics, moving back and forth with ease between crunching numbers and presenting proposals to board members. CAEs will face staffing challenges again and again. The talent is out there. The trick is finding it—and hiring it. 

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



# A Study in Risk Tolerance

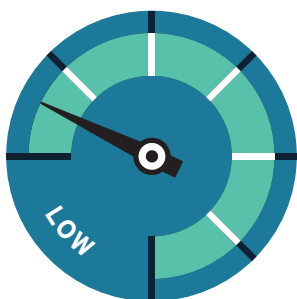
The Canada Revenue Agency is benefiting from its pilot of a tool to measure risk exposure versus tolerance.



**Louis Seabrooke**  
**Amy Felix**

**T**he general public accesses more information more frequently and expects both private and government organizations to provide more services at a proportionate rate. Each successful technological advancement to provide this information has been accompanied by numerous failures—mistakes that expose vulnerabilities and consequently entrench a risk-averse mindset within organizations. A lack of risk-taking leads to unrealized opportunities and stifled innovation. Conversely, uncontrolled risk-taking can result in disaster. Trying to find a balance between the two can lead organizations to analysis paralysis. Measuring the risks that organizations currently take and those they are willing to take can help avoid over-analysis and enable timely, informed decision-making.

In 2016, the Canada Revenue Agency (CRA), which administers tax laws for the Government of Canada and most of the country's provinces and territories, published



its Risk Tolerance Tool to quantifiably measure the maximum level of risk exposure that management was willing to accept. The objective of this tool was to provide a basis for management discussions and to inform decisions on actions related to targeted risks. Initially, the CRA used the tool internally in yearly corporate risk profile cycles. It has since been piloted in the agency’s IT security function and internal audit department with positive results.

**THE TOOL**

When approaching risk analysis, distinguishing risk exposure from risk tolerance is critical. Organizations establish risk exposure based on the likelihood that a given risk will occur and its potential impact on the organization. Risk tolerance is the maximum amount of residual risk exposure that an organization is willing to accept while working toward an expected outcome. By comparing how these concepts are quantified, management and assurance

providers can more effectively identify the risks that must be mitigated, those that do not require additional action, and even those existing in an overcontrolled environment.

**MAKE AN ACTION PLAN**

The risk tolerance portion of the tool consists of five clear tolerance criteria that are selected based on their relevance to audit engagements and their ability to be applied consistently from one engagement to the next:

- » Maturity—The level of experience the agency has dealing with the issue or risk.
- » Criticality—The level of critical service that this risk applies to the government or the CRA.
- » Sensitivity—The level of sensitivity that the CRA has toward this risk occurring.
- » Span of control—The level of control the CRA has over this risk.

- » Base profile—A consistent factor that lowers the tolerance to each risk.

The first four criteria each receive a score out of 25; the lower the number of points, the lower the organization’s tolerance for the risk. A risk that is highly critical and sensitive, and for which the organization has a large span of control, would receive few or no points for those criteria. However, a risk with which an organization has a high level of experience would contribute to a higher tolerance, receiving up to 25 points to account for the organization’s maturity. The tool adds the points for each criterion to calculate the level of tolerance for each risk. But, because the organization is not fully tolerant of any risk, the tool applies a base factor uniformly to all risks by giving 0 points out of a possible 20 points. The final score is out of 120 (see “The Risk Tolerance Model” below).

Auditors calculate the more traditional residual risk exposure by assessing

**THE RISK TOLERANCE MODEL**

This Excel chart identifies the risks, tolerance criteria, likelihood and impact, and resulting recommendation by comparing total tolerance to exposure. The tool calculates the total tolerance and exposure based on management’s inputs, and automatically populates the recommendation column.

ID	Risk Name	Maturity	Criticality: Agency or Government Priority	Sensitivity	Span of Control	Base Profile
		High (H): 25 points Medium (M): 12 points Low (L): 0 points <b>(Score /25)</b>	High: 0 Medium: 12 Low: 25 <b>(Score /25)</b>	High: 0 Medium: 12 Low: 25 <b>(Score /25)</b>	High: 0 Medium: 12 Low: 25 <b>(Score /25)</b>	<b>Base profile is always 0 (0/20)</b>
1	Risk A	<b>H</b>	<b>M</b>	<b>H</b>	<b>H</b>	<b>Base</b>
2	Risk B	<b>M</b>	<b>M</b>	<b>H</b>	<b>M</b>	<b>Base</b>
3	Risk C	<b>H</b>	<b>H</b>	<b>H</b>	<b>M</b>	<b>Base</b>



Acceptable **misalignment on risk**—a disconnect labeled “**healthy**” by most respondents—is a dangerous mindset, according to The IIA’s OnRisk 2020 report.

the risk likelihood and the risk impact and multiplying them. Note that likelihood and impact each have a maximum of 5 points. Therefore, to obtain the residual risk score out of 100, the product of the likelihood times the impact is multiplied by 4. For example, if the likelihood is 3 and the impact is 5, the residual risk exposure would be  $3 \times 5 \times 4 = 60$ . The tool then factors in the trend for a given risk by considering if it is increasing, decreasing, or stable; +20, -20, and 0 respectively. Adding the trend to the residual risk exposure results in a total risk exposure out of 120.

The tool compares total risk exposure with the total tolerance to determine if controls should be maintained, if the risk is in a caution zone, or if risk mitigation is required.

The CRA developed a slider figure alongside the risk tolerance tool to help management visualize the output of its risk analysis (see “Risk Tolerance Slider” on page 45). By inputting the exposure

and tolerance values into the slider bar, the user can quickly and clearly visualize the residual risk exposure in relation to the risk tolerance threshold and the necessary level of action. Auditors flag risks that are within the caution zone for closer observation. However, although there is no mandatory requirement for mitigation, management can choose to mitigate or monitor the risk as it sees appropriate.

One of the CRA’s priorities when developing this tool was ensuring the flexibility and adaptability of the risk criteria. Users can modify these criteria based on organizational needs and scale them to fit any type of project. Because the scoring methodology remains constant across different criteria, organizations can maintain consistency in decision-making when assessing the need for intervention. Additionally, users can modify and adjust both the set of criteria and the weight attributed to each criterion over time to better reflect the organization’s risk environment.

Therefore, although consistent criteria allow for comparability, auditors can tailor the tool to any audit phase, as long as it is consistent within that phase.

### ADDRESSING RISK

Internal audit’s use of the tool assessed the risks related to differing opinions of the audit client and audit team about the significance of a finding and internal audit’s recommendation—namely, where the client indicated no action was necessary.

The tool indicated to management that action was preferable and allowed the audit client to address the areas where risk exposure was above tolerance. Of the three risks related to the recommendation, management confirmed that one risk did not need to be mitigated. However, two risks with gaps between tolerance and exposure should be addressed with a balanced set of actions. Those actions included interim measures to mitigate a risk expected to be eliminated by a system change in a few years. Management may not have recognized the importance of acting on the risk until the system change, but the tool helped executives realize that the risk needed to be mitigated leading up to the system change.

Having audit client subject-matter experts fill out the risk tolerance tool helped them better understand the recommendation and the possible actions that they could take. This improved relationships between auditors and audit clients so clients could focus their energy on developing solutions for addressing identified gaps instead of negotiating recommendations.

By applying this stable risk-tolerance process, employees can have a consistent understanding of both the organization’s approach to risk and management’s risk mitigation criteria. This predictability also can lead to increased employee confidence in senior management’s decision-making

Total Tolerance Score /120	Likelihood	Impact	Risk Exposure Score /100	Trend ±20	Total Risk Exposure Score /120	Recommendation
37	1	3	12	0	12	Maintain Controls
36	3	3	36	0	36	Caution Zone
37	3	4	48	0	48	Mitigate



# An Exclusive Opportunity

*Join a select group of rising and distinguished internal audit professionals for a three-and-a-half-day, immersive executive development experience.*

*"It helped me be a better leader for my internal audit department."*

## 2020 VISION UNIVERSITY SESSIONS EXECUTIVE DEVELOPMENT

**Boston, MA**

June 15–18  
Omni Parker House

**San Diego, CA**

Sept. 14–17  
Kimpton Solamar Hotel

**Chicago, IL**

Nov. 2–5  
Kimpton Hotel Palomar

*Your CAE Success Story Starts Here*

**VISION UNIVERSITY**



**AUDIT EXECUTIVE  
CENTER**

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

# Clear and direct expectations about risk tolerance can help optimize risk for the enterprise over the long term, according to ISACA's State of Enterprise Risk Management 2020.

## RISK TOLERANCE SLIDER

While sliders must be created manually, they provide a quick reference of tolerance (solid black vertical line) vs. exposure (white box) for each risk and the corresponding risk response recommendation. This slider is the visual representation of the results from the tool in "The Risk Tolerance Model" chart on page 42.

Risk ID	Risk Tolerance and Residual Risk Exposure	Risk Response Recommendation
1		Maintain Controls
2		Caution Zone
3		Mitigate

and improved mitigation strategies by allowing management to concentrate on the most critical risks first.

### APPLYING THE TOOL ACROSS THE ORGANIZATION

During the pilot, internal audit management realized there are many other possibilities for using the risk tolerance tool in the audit and evaluation communities. Applying it within an organization's risk-based audit planning process can facilitate the identification and subsequent triage of potential engagements, so it could focus on those with the highest exposure above tolerance.

Similarly, incorporating it into the planning phase of an audit could simplify the scope and depth of the audit program. This, in turn, may increase the audit's effectiveness by focusing audit procedures on risks that have surpassed the caution zone.

In fact, since the first pilot in the reporting on recommendations, internal audit piloted the tool during scoping in the planning phase of one of its audits. Benefits to this approach are currently being analyzed. Also, internal

audit successfully piloted the tool to determine if an outstanding management action plan had become obsolete as a result of changes to the environment that affected the underlying risks that led to the original recommendation.

### A RISK-AWARE CULTURE

While the CRA continues to pilot and refine the risk-tolerance assessment approach within internal audit, other Canadian government departments have expressed interest in piloting the tool to identify additional applications. This has expanded intelligent risk-taking across the government. By promoting and getting employee buy-in for a more risk-aware culture, the possibilities for using the tool have become endless. [i](#)

**LOUIS SEABROOKE, CIA, CPA, CA**, is director general, Internal Audit and Evaluation Directorate, at the Canada Revenue Agency in Ottawa, Ontario, and a 2014 Internal Auditor magazine Emerging Leader.

**AMY FELIX, CIA, CPA, CA, PRINCE2**, is director, internal audit, at the Canada Revenue Agency in Ottawa.



**VISIT**  
[Internal Auditor.org](https://www.iaa.org)  
 to view risk tolerance scoring criteria and guidance, and risk likelihood and risk impact scales.





# Bringing clarity to the *foggy* world of AI

In unveiling the U.S. government's updated National Artificial Intelligence (AI) Research and Development Strategic Plan last June, U.S. Chief Technology Officer Michael Kratsios framed the reality many organizations face with AI. "The landscape for AI research and development (R&D) is becoming increasingly complex," Kratsios said, noting the rapid advances in AI and growth in AI investments by companies, governments, and universities. "The federal government must therefore continually reevaluate its priorities for AI R&D investments to ensure that





Strategy and governance should be internal audit's focus in assessing artificial intelligence systems.

Kevin M. Alvero  
Wade Cassels

Illustration by Sean Yates

Base photograph by Amanda Carden/Shutterstock.com



investments continue to advance the cutting edge of the field and are not duplicative of industry investments.”

Organizations are indeed investing in AI. About one-third of companies in Deloitte’s most-recent State of AI in the Enterprise survey said they were spending \$5 million or more on AI technologies in fiscal year 2018. Moreover, 90% expected their level of investment to grow in 2019. These investments are

learning, image recognition, natural language processing, cognitive computing, intelligence amplification, cognitive augmentation, machine augmented intelligence, and augmented intelligence. Additionally, some people include robotic process automation (RPA) under AI because of its ability to execute complex algorithms. However, RPA is not AI because bot functions must adhere strictly to predetermined rules.

When considering which technologies fall under the umbrella of AI for internal audit purposes, it is important to understand how the organization defines it. For that reason, ISACA’s Auditing Artificial Intelligence guide recommends auditors communicate proactively with stakeholders to answer the question, “What does the organization mean when it says ‘AI?’” This alignment can help auditors manage stakeholder expectations about the audit process for AI. Moreover, it may tell auditors whether the organization’s definition of AI is broad enough—or narrow enough—for it to perceive risk in the marketplace.

## With so much on the line, organizations must invest the right resources in the right places to capitalize on AI.

occurring across all facets of business, from production and supply chain to security, finance, marketing, customer service, and internal audit.

With so much money on the line, organizations must invest the right resources in the right places to capitalize on AI. But with the technology evolving rapidly, it’s not clear how they can accurately assess AI-related risks and ensure that projects are consistent with the organization’s mission, culture, and technology strategy. In this sometimes-foggy environment, internal audit can be a valuable ally by focusing on whether the organization has a sound AI strategy and the robust governance needed to execute that strategy (see “AI Deployments More Difficult Than Expected” on page 11).

### DEFINING AI

The definition of *artificial intelligence* is somewhat ambiguous. There is not universal agreement about what AI is and what types of technologies should be considered AI, so it’s not always clear which technologies should be in scope for internal audits.

Technologies that fall into the realm of AI include deep learning, machine

### START WITH STRATEGY

However the organization defines AI, most guidance agrees that internal audit should focus its audits on the organization’s AI strategy and governance. Without a clearly articulated and regularly reviewed strategy, investments in AI capability will yield disappointing results. Worse, they could result in financial and reputational damage to the organization. Internal audit should confirm the existence of a documented AI strategy and assess its strength based on these considerations:

- ➔ *Does the strategy clearly express the intended result of AI activities?*

The strategy should describe a future state for the business and how AI is expected to help reach it, as opposed to AI being viewed as an end unto itself.



# The use of AI in anti-fraud efforts will almost triple in the next two years, according to ACFE's Anti-fraud Technology Benchmarking Report 2019.

- ➔ *Was it developed collaboratively between business and technology leaders?* To provide value, AI endeavors must align business needs and technological capability. Auditors should verify whether a diverse group of stakeholders are providing input.
- ➔ *Is it consistent and compatible with the organization's mission, values, and culture?* With expanding use of AI comes new ethical concerns such as data privacy. Auditors should look for evidence that the organization has considered whether planned AI uses are consistent with what the organization should be doing.
- ➔ *Does it consider the supporting competencies needed to leverage AI?* Successfully implementing AI requires support and expertise around IT, data governance, cybersecurity, and more. These areas should be factored into the organization's AI strategy.
- ➔ *Is it adaptable?* While the cadence will vary by organization, key stakeholders should review the AI strategy periodically to confirm its viability and to ensure it accounts for emerging threats and opportunities.

Organizations need their internal audit departments to ask these types of questions, not just once, but repeatedly. Research shows that organizations want their internal audit departments to be more forward-looking and provide more value in assessing strategic risks. Regarding supporting competencies, board members and C-level leaders are most concerned that their existing operations and infrastructure cannot adjust to meet performance expectations among "born digital" competitors, according to Protiviti's Executive Perspectives on Top Risks 2019 report. As such, internal auditors can provide

assurance that the organization's AI strategy is appropriate and can be carried out realistically.

## **PAY ATTENTION TO DATA GOVERNANCE**

As with any other major system, organizations need to establish governance structures for AI initiatives to ensure there is appropriate control and accountability. Such structures can help the organization determine whether AI projects are performing as expected and accomplishing their objectives. The problem is that it's not yet clear what AI governance looks like.

According to a 2018 Internal Audit Foundation report, *Artificial Intelligence: The Data Below*, "There is not a template to follow to manage AI governance; the playbook has yet to be written." Even so, the report advises internal auditors to assess the care business leaders have taken "to develop a robust governance structure in support of these applications." That exploration should start with the data.

Big data forms the foundation of AI capability, so internal audit should pay special attention to the organization's data governance structure. Auditors should understand how the organization ensures that its data infrastructure has the capacity to accommodate the size and complexity of AI



**Big data forms the foundation of AI capability, so internal audit should pay attention to data governance.**

activity set forth in the AI strategy. At the same time, auditors should review how the organization manages risks to data quality and consistency, including controls around data collection, access rights, retention, taxonomy (naming),



and editing and processing rules. They also should consider security, cyber resiliency, and business continuity, and assess the organization's preparedness to handle threats to the accuracy, completeness, and availability of data.

AI value and performance also depend on the quality and accuracy of the algorithms that define the processes that AI performs on big data. Documented methodologies for algorithm development, as well as

functions. To audit the technology effectively, internal audit functions must have or acquire sufficient resources, knowledge, and skills. That doesn't mean they need expert-level knowledge on staff, though.

Obtaining these capabilities has proved to be challenging. According to The IIA's 2018 North American Pulse of Internal Audit, 78% of respondent chief audit executives indicated it was very difficult to recruit

**Soon it will be difficult to find an area of the business that does not leverage AI in some way.**

quality controls, must be in place to ensure these algorithms are written correctly, are free from bias, and use data appropriately. Moreover, internal audit should understand how the organization validates AI system decisions and evaluate whether the organization could defend those decisions.

In addition to governance around data and AI algorithms, internal audit should examine governance structures to determine whether:

- ➔ Accountability, responsibility, and oversight are clearly established.
- ➔ Policies and procedures are documented and are being followed.
- ➔ Those with AI responsibilities have the necessary skills and expertise.
- ➔ AI activities and related decisions and actions are consistent with the organization's values, and ethical, social, and legal responsibilities.
- ➔ Third-party risk management procedures are being performed around any vendors.

#### AI GAINS MOMENTUM

AI poses challenges that make auditing it daunting for many internal audit

individuals with data mining and analytics skills. Nevertheless, the internal audit function should work to steadily increase its AI expertise through training and talent recruitment.

However, success in auditing AI does not depend directly on technical expertise. Instead, auditors must be able to assess strategy, governance, risk, and process quality—all things they can bring from an independent, cross-departmental point of view.

The sooner internal auditors do this, the better, because AI, in all its various forms, is gaining momentum. Soon, it will be difficult to find an area of the business that does not leverage it in some way. And although the constantly evolving technologies and risks can be dizzying, internal audit can provide sound assurance that the organization is pointing its AI investments in the right direction. [la](#)

**KEVIN M. ALVERO, CISA, CFE**, is senior vice president-internal audit at Nielsen in Oldsmar, Fla.

**WADE CASSELS, CIA, CRMA, CISA, CFE**, is a senior auditor at Nielsen.





Against a backdrop of an over-leveraged economy, there is increased impetus for internal audit to assess financial risk.

Brendan Scott

**A** decade of unprecedented loose monetary policy designed to stimulate the global economy has been a godsend for businesses. Cheap financing has allowed companies to invest in growth and reward shareholders with share buy-backs, pushing stock markets to record highs. Recent years have been good to CEOs. Meanwhile, increasingly sophisticated automation and a belief that financial risks were relatively well-understood, compared with some emerging audit areas, mean that many internal audit functions had put financial risk on a back burner. But accommodating financial conditions also have allowed risks to build. “In advanced economies, corporate debt and financial risk-taking have increased, the creditworthiness of borrowers has deteriorated, and so-called leveraged loans to highly indebted borrowers continue to be of particular concern,” Tobias Adrian, financial counselor of the International Monetary Fund, told an audience in April 2019 at the launch of the most recent Global Financial Stability Report.

It is hardly surprising then that financial risk has moved back toward the top of the list of business risks cited by chief audit executives in the Risk in Focus 2020 report, a collaboration among IIA institutes in Belgium, France, Germany, Italy, the Netherlands, Spain, Sweden, and the United Kingdom and Ireland. Nearly one-third of respondents listed it in their top five risks. As news headlines highlight a plethora of concerning indicators—anti-globalist trade policy, weak manufacturing data, the inversion of the yield curve on various government bonds,

# ON THE MONEY

time to revisit financial risk

decelerating global growth, and other recessionary signals—boards and audit committees are increasingly likely to seek assurances that financial risk is being mitigated effectively.

### COMING FULL CIRCLE

The management of financial risk on a day-to-day level lies ultimately with the finance function. Called the treasury in many countries, the finance function manages the business' liquidity and monitors cash inflows and outflows, current and projected, to ensure sufficient funds are available to support the company's operations and excess cash is invested effectively. Although finance is fundamental to the success of the business, it's useful for internal auditors to remember that some board members may have blind spots in their knowledge and awareness of the basics, particularly when it comes to the company's balance sheet.

“Nonfinance directors tend to be less familiar with the balance sheet and the cash flow statement than the profit and loss (P&L). By extension, they are typically less comfortable with the balance sheet lexicon, such as the true meaning of assets, liabilities, and equity,” warns Steve Giles, a course leader at the London-based Institute of Directors on its Finance for Non-finance Directors learning program. “They are aware of concepts such as ‘cash is king,’ but do not readily translate this to the importance of managing working capital and the cash cycle in their business.” He adds that the “corporate killer” is rarely a lack of profits, but the business' inability to pay debts when they are due.

This is why internal auditors in many sectors may now be urging boards to think seriously about market conditions and financial risks. In times of growth, when markets are calm,

auditors conducting routine finance audits should watch for signs that the finance function is becoming complacent or that financial risk management standards are slipping. But when rising trade tensions combine with the highest-ever levels of corporate debt, they should scrutinize all aspects of financial risk, as earnings are likely to be under pressure.

“Trade wars are bad for everybody. Their ultimate impact is a movement toward lower earnings,” says Pat Leavy, CEO at FTI Treasury, a Dublin-based treasury outsourcing and audit firm. “This combined with the presence of leverage obviously increases risk, but, from an audit perspective, when we're looking at individual companies, we need to understand the data we see.”

Leavy explains that although gross corporate debt has risen, internal audit should focus more on net corporate debt. The risk is lower when corporations have high debt and also high levels of cash and liquid assets—a good example is the airline industry. “The focus should be on debt repayment capability, rather than profits and earnings before interest, tax, depreciation, and amortization alone,” he says. “What we're really looking at is cash generation.”

### QUALITIES OF A GOOD FINANCE FUNCTION

So, what does a good finance function look like, and what should internal auditors consider when they audit it? Leavy likens the quality of the finance function to Maslow's hierarchy of motivation. At the bottom of the pyramid is the quality of the infrastructure in place to manage the function: the resources and people, the competency of those people and the quality of the technology infrastructure, including any automation, and the commitment to the processes that are in place. The next level up is the control environment, the segregation of duties, the





30% of CAEs cite financial risks as a top 5 risk to their organization, while 6% rate it their top risk, according to Risk in Focus 2020, released by eight European-based IIA institutes.

checks and balances, the flow of information, and compliance with those safety measures.

“As you move up the pyramid, it becomes more subjective,” Leavy says. “Success at the next level depends on getting the right balance between developing strategy and managing the operations.” Finance functions often spend 10% of their time on strategy and 90% on managing operations and getting the day-to-day work done. “In reality, getting the treasury strategy right can have a much more significant impact on the business,” he says.

Finance functions often operate in isolation from the business and can be reactive. Ideally, they should be proactive and able to anticipate and be part of the corporate decision-making process. In this kind of finance function, the group treasurer moves up the value chain, working directly with the chief financial officer and risk committee to help define and achieve the corporate strategy.

#### WHERE AUDITS FOCUS

Similarly, Leavy says, finance audits tend to focus on the lower (although essential) rungs—operations controls and governance—and less on the finance function’s strategy and how it enables the overarching corporate strategy. His points are echoed by Angela O’Hara, who spent five years as group assurance and risk director at an FTSE 100 chemicals and technology company before recently stepping into a director role. She also sits on the finance and general purposes committee of the Royal Veterinary College. O’Hara says limited resources meant that the finance audit she oversaw was outsourced and focused almost entirely on the basics.

“That audit looked at processes and governance, but not at the impact of the financial risks in the business and the treasury’s role in relation to those risks,” she explains. Auditors assessed how well the finance function managed

bank accounts, and whether it reviewed the business’ credit rating and funding arrangements regularly, as well as access rights for critical systems, the payment and processing platform, and foreign exchange (forex) trading. “But it didn’t look at, for example, whether there had been a forex gain or loss, what led to that, and whether there should be changes to the roles and responsibilities associated with that,” she says.

**In times of growth, auditors should watch for signs that the finance function is becoming complacent.**

O’Hara says it is common for internal audit to assess how a function is set up, but there is additional value to add in assessing that function’s effectiveness and what it means for the business. Reviewing structure, governance, policies, procedures, and key controls is fundamental. But, building on that, internal audit needs to challenge the function and its assumptions, even if it is not an expert on forex hedging or financing strategies.

“It’s not a case of suggesting that what the treasury is doing is incorrect, but of raising questions that need to be considered in a rational and objective manner,” Leavy adds. “And also of considering alternative approaches that might be more suitable and being open to that dialogue.”

Alistair Smith, U.K. internal audit, risk, and control director at EDF Energy, says the transactional and frequent nature of finance activities makes them suitable for automation. However, in organizations using this kind of technology, internal audit should consider how key person risks and segregation of duties are managed. Another key risk, especially in long-established finance



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

# Mission Critical Thinking

EXPLORE IMPERATIVE QUESTIONS, DISCOVER ESSENTIAL ANSWERS.



In this significantly restructured version, *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value, 7th Edition*, 10 internal audit thought leaders tackle the challenges of defining what it takes to fulfill internal audit's mission of enhancing and protecting organization value. In short, Sawyer's is universally considered the single most important resource to help internal auditors of all levels and sectors think critically about changes in the environment and business landscape, as well as the evolution of the audit plan and services that internal audit must develop and deliver. Sawyer's is critical to delivering the mission of internal audit.

**Think critically, then fulfill your mission.**

Order Today! [www.theiia.org/Sawyers](http://www.theiia.org/Sawyers)

  
INTERNAL AUDIT  
FOUNDATION™



42% of organizations increased cash reserves in the past year, possibly in response to uncertain economic conditions, according to *Treasury & Risk's* 2019 Cash Management Survey.

teams, is over-familiarity with the business, which can lead to “passive checking” of approvals for things like setting up new bank accounts. The best finance functions also will be able to provide metrics to demonstrate how they add value, whether through their forex hedging strategy or by optimizing financing.

### STANDARD DEVIATION

Internal audit may not be able to predict whether the economy will go into recession, but there are more mundane matters that should be well-understood and managed. Changes to International Financial Reporting Standards (IFRS) accounting standards, for example, can catch finance functions off guard in companies that are required to comply with them.

IFRS 15, which came into effect in January 2018, requires that businesses subject to IFRS recognize revenues only when they are collected and not when customer contracts are signed, a change that has affected the top lines of high-profile companies. IFRS 16, which went live in January 2019, also has caused some turbulence. The new standard requires that payments made on operating leases—used for property and equipment in asset-heavy industries—must for the first time be reported as a liability on balance sheets. In September, FTSE 100 construction rental business Ashstead reported a huge jump of £1.4 billion (\$1.8 million) in its net debt to £5.2 billion (\$6.8 million) in the second quarter, well over half of which directly resulted from the accounting switch.

“The one we are coming across more and more is IFRS 9 on the impairment of intercompany loans,” Leavy cautions. “There may be a requirement to calculate potential credit losses and include that as a repairment charge on intercompany debt. So suddenly there can be a movement on the P&L as the result of an accounting amendment,


and intercompany lending is a bread-and-butter issue for every large corporation with an international footprint.”

Another consideration for global businesses is the finance function’s strategy of cash pooling, whereby the debit and credit balances of numerous subsidiaries’ accounts are aggregated, allowing them to centralize group liquidity management. This can improve the

## Changes to International Financial Reporting Standards can catch financial functions off guard.

interest terms they are offered when they raise finance and optimize cash flow within the group.

Certain jurisdictions, however, place restrictions on the strategy. “Notional cash pooling,” a virtual rather than physical concentration of cash, is prohibited in Argentina, Brazil, Chile, India, Mexico, Sweden, Turkey, and Venezuela, in favor of physical pooling. India has even stricter rules that forbid cross-border physical pooling. Internal audit departments working across geographically diverse businesses should bear in mind the complications that can arise from subsidiaries that may sit outside of the pool.

“You need to look at those outliers as well as at the big risks,” O’Hara says. “Clearly there is a big gross risk in the central treasury function, but each of the outliers could impact the P&L.” 

**BRENDAN SCOTT** is a freelance writer based in London.

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



# Board Perspectives

BY MATT KELLY

## THE BOARD AND WHISTLEBLOWERS

Corporate boards' need for a strong, durable process to oversee allegations of executive misconduct has never been more clear.



DOTTY HAYES



DAVID DIAMOND



CHARLOTTE VALEUR

In 2018 the CEO of Barclays, Jes Staley, was castigated by British regulators for trying to unmask a whistleblower who had raised concerns about one of Staley's top lieutenants. Barclays' board clawed back a £500,000 bonus from Staley, and regulators fined him £640,000. Regulators in New York then hit Barclays, itself, with another \$15 million penalty.

The year prior, life sciences company Bio-Rad had to pay nearly \$8 million to former general counsel Sanford Wadler after he reported fears of possible bribe payments to government officials in China. The company sacked Wadler, who filed a whistleblower retaliation lawsuit.

Bio-Rad and Barclays are especially noteworthy because in both cases, the whistleblowers' allegations were later determined to be unfounded. An arbitrary approach to handling whistleblowers is what got those

companies into hot water. In our highly regulated, highly litigious, highly transparent world, it always is. Hence the need for rigor—and the need for boards to assure that rigor exists.

"It's important to set up a process [for addressing whistleblower complaints] in advance because you have to take every one of these issues seriously," says Dotty Hayes, a former CAE at both Intuit and Hewlett-Packard and now chair of the board of directors at First Tech Federal Credit Union in San Jose, Calif., and a board member and audit committee chair at a range of organizations. "You can't do it haphazardly."

That point is true even if the allegation doesn't seem credible, and even if it's proven wrong, Hayes says. The last thing a board wants is to improvise a response.

### **Be Disciplined; Be Independent**

The good news is that truly grave whistleblower

reports—allegations so serious that the board should oversee them, and should do so immediately—seem to be rare. "In my experience, if you have one or two a year that are significant and require high priority, that's a lot," says David Diamond, former head of internal audit at Lionsgate Entertainment, and now audit committee chair for The Daily Breath, a chain of Pilates studios in Brazil and the U.S. Likewise, Charlotte Valeur, CEO of the Global Governance Group and currently a director on seven boards, says that in 14 years of working in board governance, she has encountered only two instances of whistleblower allegations so serious that only the board could address it.

Again, so what? Boards don't know the veracity of a whistleblower allegation when the report first arrives. So establishing a consistent, disciplined, objective process to evaluate whistleblower reports is paramount.

READ MORE ON [STAKEHOLDER RELATIONS](#) visit [InternalAuditor.org](http://InternalAuditor.org)



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

“Independence on boards is key for whistleblowing,” Valeur says. “If you don’t have independent board members who can deal with it—and *will* deal with it, truly independently—everybody is at risk. The whistleblower is at risk, and the company is at risk.”

In truth, that triage process is a nuanced tango between board and management. Boards might *receive* reports, but they should not *investigate* reports; that duty should go to trained professionals: internal audit, the compliance or legal team, human resources (HR), or even outside counsel. Even in grave scenarios such as allegations of CEO misconduct, the board should oversee that investigations are happening and moving forward—but not *participate* in the investigation, itself. “The last thing I want to do is be the investigator,” Hayes says.

Conversely, management receives lots of reports, and might even investigate many of them without troubling the board. That’s fine, so long as all parties have a clear understanding of which reports *should* be escalated to the board right away.

So what should that process look like? Who’s involved in the triage? Typically a large company will outsource its whistleblower hotline; that’s one layer of independence. A

## Boards should welcome reports based on secondhand information.

whistleblower might be able to select categories of complaint (accounting fraud, employee bullying, discrimination, theft, and so forth), or specialists at the outsourced hotline provider could assign one based on certain key phrases, issues, or even names the whistleblower might include.

A critical question is which categories of complaint should automatically go to the board, even if the board then bats the issue right back to audit, legal, or compliance for further action. For example, anything that mentions corporate accounting, compliance violations, or CEO misconduct should go to the board. If the issue involves personal misconduct rather than financial, consideration by a risk or governance committee might be the best option.

Should the accused be informed of the allegations against him or her? Generally no, although some privacy rules in Europe can make that a complicated question best left to professional investigators. And should a company try to unmask a whistleblower? Pretty much never, since that action is a whisker away from retaliation and violates the spirit of following the facts wherever they may lead. (“It’s irrelevant,” Valeur says of the idea.)

And regardless of how any specific allegation is investigated, boards still need a process to oversee whistleblower reporting holistically. Valeur, for example, says she wants regular briefings on the total number of reports, the issues they involve, substantiation rates, and so forth.

“All companies over a certain threshold should have a mature process,” Diamond adds. “If you don’t, in this day and age, you’re way behind.”

### Speaking of Substantiation...

Boards might also be surprised at this news: Whistleblower reports based on secondhand knowledge—that is, information passed along to the whistleblower from someone else; or that the whistleblower discovers by finding evidence of misconduct, without witnessing the act directly—tend to be more reliable than reports from people with *firsthand* knowledge. So says research from The George Washington University and the University of Utah, where academics studied 2 million whistleblower reports filed at more than 1,000 companies from 2004 through 2017. They found that management was 48% more likely to substantiate whistleblower reports based on secondhand information. Those reports

were more likely to be about accounting and business integrity issues, too; while firsthand reports are more often about HR issues.

That makes sense when you think about it. People filing firsthand reports are usually claiming that they have

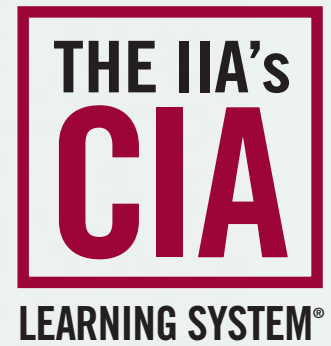
somehow been wronged personally—and, yes, some portion of those reports will be false, or based on hot-headed judgments that don’t hold up under scrutiny.

Whistleblowers with secondhand information, however, are claiming that something in the company is amiss. You typically wouldn’t do that unless you care about the organization. And if you care about the organization, you’re probably not involved in the misconduct, so it’s more likely you have fragments of evidence. In other words, boards should welcome whistleblower reports based on secondhand information, even though that means more investigative spadework to find the truth.

“Many times the report needs to be ferreted out,” Diamond says. “A lot more details need to be derived to understand the full significance of the report.”

True, but investigations are the subject for a different day. The importance of establishing a process to oversee whistleblower allegations in an objective, disciplined way and follow the facts where they lead—that advice is irrefutable. [la](#)

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



# 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)



2018-0267





BY J. MICHAEL JACKA

## DRUNK AND IN CHARGE OF A BICYCLE

Much of the fun in audit work comes from exploring, experimenting, and enjoying the journey.

In his excellent book *Zen in the Art of Writing*, science-fiction author Ray Bradbury features an essay titled “Drunk, and in Charge of a Bicycle.” Bradbury uses the essay to discuss his approach to writing, including this choice snippet:

*“That is the kind of life I’ve had. Drunk, and in charge of a bicycle, as an Irish police report once put it. Drunk with life, that is, and not knowing where off to next. But you’re on your way before dawn. And the trip? Exactly one half terror, exactly one half exhilaration.”*

What if we were to perform our audits that way? What if we started without knowing everything? What if we had an idea of how to approach a risk, but found ourselves on our way before dawn without knowing where we were headed? What if we simply trusted our intuition, our skills, and our professionalism to lead us to the correct destination? Imagine auditing with no hours spent preplanning on preplanning, no interminable meetings about the

meeting about the meetings, no second-guessing before the first guess has been made, and no excruciating detail of dotting every “i” and crossing every “t.” Instead, engagements would involve exploring the mostly unknown and learning what we do not know, what we need to know, and what will provide the most value to the organization.

And here’s another quote from Bradbury’s essay: “By the time many people are fourteen or fifteen, they have been divested of their loves, their ancient and intuitive tastes, one by one, until when they reach maturity there is no fun left, no zest, no gusto, no flavor.”

In spite of what some people say about the internal audit profession, it can be a lot of fun. I’ve been in it for more than 30 years—no one without masochistic tendencies of a type I cannot fathom stays in a profession that long unless they are having fun. And I’m still having fun because there is still so much to learn, so much to explore, and so much potential and opportunity.

Practitioners would do well to quit trying to make sure everything is perfect and instead just enjoy the job. Most of the fun I have had in internal auditing came when I was exploring. And I’m willing to wager the bicycle mentioned above that, upon close examination, that’s when the majority of internal auditors have the most fun too. An important part of that fun is diving into the work, without fear or worry. As nature essayist John Burroughs advised, “Leap and a net will appear.”

Some of my best work as an auditor, and some of the most fun I had, came when I was not enmeshed in the details—when I was allowed to experiment, explore, and leap, letting the work lead where I least expected. In other words, it occurred when I was, metaphorically, drunk and in charge of a bicycle. [\[a\]](#)

---

**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)

## THE EVOLUTION OF TALENT MANAGEMENT

As the organization evolves, so, too, should internal audit's acquisition and retention strategies.



**SANDY PUNDMANN**  
U.S. Internal Audit  
Leader  
Deloitte



**SAM AINA**  
U.S. Internal  
Audit Leader for  
Technology, Media, and  
Telecommunications  
Industries  
Crowe

### How should talent management strategies be evolving?

**PUNDMANN** Organizations are looking for consultative, critical-thinking advisors who understand all sides of the business—from strategy and finance to cybersecurity and culture risk management—for their internal audit teams. As organizations evolve, so do their talent strategies. We're seeing more organizations using rotational or guest auditor programs to engage professionals with diverse areas of expertise outside of internal audit to help address the varied challenges that core internal audit work presents. Because of the variety of challenges internal auditors face, many leading organizations' talent development strategies include internal audit as a key career development assignment.

**AINA** Today's business environment disruption is driven by technological advancements and generations that

know technology and its rapid evolution as the norm. Talent management strategies need to demonstrate that the organization embraces, and is well-positioned to take advantage of, disruptive technologies. These strategies also need to evolve to a talent pool that thrives on change by providing a uniquely diverse set of experiences through opportunities within and outside the functions for which the talent was recruited.

### With the growing impact of digitalization, what new skills should CAEs be looking for in candidates?

**AINA** It depends on where chief audit executives (CAEs) see their organization and industry trending in terms of technology innovation and the associated regulations and risks that CAEs will need to audit. Though not new skills, adaptability, resilience, and innovation to facilitate change are critical for success. How have candidates

demonstrated resilience amid change—system changes, policy changes, schedule/deadline changes, team changes, project changes, significant life changes, etc.? Have they driven change through innovation, not just by providing interesting findings and recommendations, but by improving the effectiveness of their own department? CAEs also should look for candidates with a broad understanding of business, with a consultative mindset. And, there is always an expectation that every function will do more with less through the use of technology. IT audit backgrounds are no longer restricted to traditional IT audit experience and information systems degrees. Rather, competence, skills, and experience in computer science/programming, data science and analytics, robotic process automation, cybersecurity, and privacy compliance are needed.

**PUNDMANN** We're seeing increasing demand for internal

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



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

audit teams staffed with people with a diverse set of skills and “purple people” who combine the “red” skills of sophisticated data analysis and architecture backgrounds with the “blue” skills of business acumen, design thought, and political sense. CAEs are looking for analytics and digital capabilities, along with critical thinking and business acumen, and Agile, collaboration, and problem-solving skills.

### What importance should be placed on internal audit certifications in identifying potential candidates?

**PUNDMANN** While internal audit certifications are a relevant part of the discussion for internal audit staffing, it's key to look at the full team's composition. If all or none of the team has an internal audit background, there's a problem. But, if the team comprises a mix of people holding various certifications—Certified Internal Auditor (CIA) for internal audit skills, Certified Public Accountant (CPA), Certification in Risk Management Assurance, and others—the team is likely well-positioned to help accomplish business objectives.

**AINA** I hold the CIA, CPA, and Certified Fraud Examiner certifications, but my experiences, skills, and relationships are even more important. CAEs should be thinking outside the internal audit box, because the world is progressively eliminating that box altogether. The right talent will pick up on internal audit methodology and standards and can readily gain the required experience to achieve an internal audit certification; however, innovation, adaptability, commitment, accountability, and leadership are far more challenging to develop.

### How does the gig economy affect talent strategies?

**AINA** There's a growing desire for greater flexibility in when and how people work, as evidenced by the gig economy. Coupled with the talent pool's desire for diverse experiences, it's another part of the disruptive business environment. Gig economy dynamics can manifest through more leaves of absence, flexible work arrangements, and turnover. CAEs should anticipate this and develop a methodology that adapts to these dynamics. They should embrace the gig economy impact by recruiting talent who can help them adjust their internal audit talent management approach to further explore, develop, and deploy strategies to engage and retain the current talent pool. Additionally, part of having a flexible internal audit team and talent management strategy should include strategic partners and trusted advisors who can promptly compensate for temporary or long-term skill gaps and manpower needs.

**PUNDMANN** Internal audit groups use a mix of resourcing models to deliver their audit plans, and as specialization is in high demand, it's easy to understand why. Eighty percent of the global CAEs Deloitte recently surveyed said specialist skills, which are a great use of a “gig” worker, drove their use of

alternative resourcing models. For example, a full-time equivalent employee may not be needed for an environmental audit. Just-in-time resources, as the gig economy can provide, can help as expectations of internal audit become more complex.


### What retention strategies can CAEs implement to make their departments attractive to potential applicants?

**PUNDMANN** Increasingly more professionals—younger generations, but also the more experienced among us—are purpose-driven and want to make an impact. Internal audit offers that opportunity with every project that looks at some aspect of the business, evaluates it, and recommends what should be done. Learning a business through varied work in an independent, but team-based, role that affords the opportunity to communicate with the organization's leaders is attractive to those interested in making a difference.

**AINA** Involving internal audit in facilitating change while embracing and adapting to emerging technology risks will always be key. CAEs should recognize and reward innovation in their departments. That can naturally facilitate diversification of experience for top talent to keep them engaged. Organizations can further diversify the experiences available through rotational programs within and outside internal audit. Nimble and flexible methodologies and work environments are also attractive to a talent pool that would rather not get boxed in. Finally, a family feel in the function, where the office isn't just a job but rather a place where they feel at home, can go a long way in retaining personnel. Quality of life is a strategic talent influencer in today's business environment.

### What are some best practices for developing existing team talent?

**AINA** On-the-job training and learning are far better retained and engrained than classroom and coaching. Therefore, rotational programs go beyond talent retention and into developing existing talent. Coordinating opportunities for existing talent to work with personnel in other functions who possess skills and competencies that internal audit lacks, enables them to bring back the knowledge to benefit internal audit. Additionally, CAEs should challenge existing team members with new projects and opportunities.

**PUNDMANN** Leveraging Agile principles is great for developing existing team talent. CAEs build on new ways of engaging teams such that the team collectively has the knowledge, but the group iterates solutions and reflects on lessons learned after projects close. It helps develop critical-thinking skills. Of course, it doesn't hurt to have a robust training and development program to nurture the team, as well. If the organization is moving to the cloud or is pursuing another major change, internal audit needs training to get up to speed on it. 





# CRUISE

into internal audit

2020 IIA INTERNATIONAL CONFERENCE  
20–22 July / Miami, Florida

**Experience** today's top presenters and a world-class program, featuring 8 educational tracks with more than 60 sessions to choose from.

**SPANISH SPEAKING TRACK OFFERED!** The IIA will be offering a Spanish Language track. And, if you bring a group of 100 or more attendees from your region, translation for the general sessions will be included as well.

**Register today** and save! [ic.globaliia.org](https://ic.globaliia.org)





# IIA Calendar



## IIA CONFERENCES

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

**MARCH 16-18**  
**General Audit Management Conference**  
 ARIA Resort  
 Las Vegas

**APRIL 5-7**  
**Leadership Academy**  
 Disney Yacht Club Resort  
 Orlando, FL

**JULY 19-22**  
**International Conference**  
 Miami Beach Convention Center  
 Miami

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

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

**SEPT. 16-17**  
**Women in Internal Audit Leadership**  
 Omni Shoreham  
 Washington, DC

**NOV. 2-4**  
**All Star Conference**  
 MGM Grand  
 Las Vegas

## IIA TRAINING

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

**MARCH 3-6**  
**Multiple Courses**  
 Tulsa

**MARCH 10-19**  
**Critical Thinking in the Audit Process**  
 Online

**MARCH 18**  
**Fundamentals of Internal Auditing**  
 Online

**MARCH 24-27**  
**Multiple Courses**  
 Boston

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

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

**MARCH 31-APRIL 9**  
**Advanced Risk-based Auditing**  
 Online

**APRIL 7-10**  
**Multiple Courses**  
 New York

**APRIL 13-16**  
**Statistical Sampling for Internal Auditors**  
 Online

**APRIL 20-29**  
**Root Cause Analysis for Internal Auditors**  
 Online

**APRIL 21-24**  
**Multiple Courses**  
 Orlando, FL

**APRIL 21-30**  
**Cybersecurity Auditing in an Unsecure World**  
 Online

**MAY 4-13**  
**Fundamentals of Internal Auditing**  
 Online

**MAY 5-14**  
**Audit Report Writing**  
 Online

**MAY 12-13**  
**Data Analysis for Internal Auditors**  
 Online

**MAY 12-15**  
**Multiple Courses**  
 Washington, DC

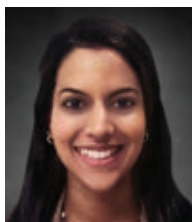
**MAY 18-20**  
**IT General Controls**  
 Online

**MAY 19-22**  
**Multiple Courses**  
 Chicago

**MAY 19-28**  
**Fundamentals of Risk-based Auditing**  
 Online

**MAY 27**  
**Fundamentals of Internal Auditing**  
 Online

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



BY NIRA KOHLI

## SEEING THE BIGGER PICTURE

A willingness to ask “why” is essential to fully appreciating our purpose in the organization.

Among questions children ask of adults, perhaps the most common is, “Why?” When told, “Clean your room,” “Do your homework,” or “The sky is blue,” children often respond “But why?” Then as we age, our innate curiosity decreases and conformity and harmony become a greater priority. We fear asking why may be interpreted as provocation, disrespectful, or even a waste of time. Our worries intensify, and the desire to fit in can overwhelm our curiosity.

For internal auditors, asking why is vital to professional development and success. It helps us understand the organization — not only our role in it, but the greater purpose we serve and contributions we provide. Asking why is necessary for seeing the bigger picture of our work.

Effective internal auditing requires a questioning mindset. Audit leaders, of course, need to communicate project goals and explain how they serve client objectives and contribute to the organization. Even so, encouraging employees to

ask why, as well, helps them obtain a better understanding of each assigned task and a greater appreciation for its significance. Plus, increased engagement empowers and motivates employees, helping ensure everyone is energized and focused.

Individual empowerment enables employees to take ownership for their work, thereby cultivating a sense of pride. They view project success not just as a win for the organization, but as a personal achievement. Continuously encouraging employees to ask why and provide feedback helps sustain that sense of pride. And by doing so, managers provide team members a voice on decisions that affect projects. The resulting employee buy-in can lead to improved work quality and interpersonal relationships, and better alignment with client needs.

Asking why can also increase camaraderie and collaboration. When auditors inquire about how each person’s role impacts a project or client, they develop a better appreciation for other members of the team. Increased awareness of team members’

roles can foster mutual respect and enhance cohesion. And when employees respect one another, it stimulates knowledge exchange as team members become more comfortable sharing ideas with one another, thereby helping to reduce team conflict and nurture employee growth.

While visiting the National Aeronautics and Space Administration headquarters, U.S. President John F. Kennedy asked a janitor what he did at the agency. The janitor replied, “I’m helping put a man on the moon.” The janitor realized his part in accomplishing the overall objective. To some people, the janitor was cleaning the building, but he understood his role in helping make history. This greater understanding illustrates the depth of commitment and sense of purpose employees can possess when they see the bigger picture — often stemming from a sense of curiosity and a willingness to ask why. [\[E\]](#)

**NIRA KOHLI** is a senior audit consultant based in the U.S. with experience working for multinational companies.

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



## 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)

**GET THE DATA.  
GET THE DEFINITIONS.  
GET THE DIRECTION.**



**Get *OnRisk* 2020:**

*A Guide to Understanding, Aligning, and Optimizing Risk*, a one-of-a-kind report that brings together risk perspectives from the board, the C-suite, and CAEs; analyzes how their perceptions differ; and provides valuable insights on what that means for organizations.

**Download your free copy today.**

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

