

# Ia

INTERNAL AUDITOR

DECEMBER 2018

A PUBLICATION OF THE IIA

Right-sizing Internal Audit

The Rise of Artificial  
Intelligence and Robotics

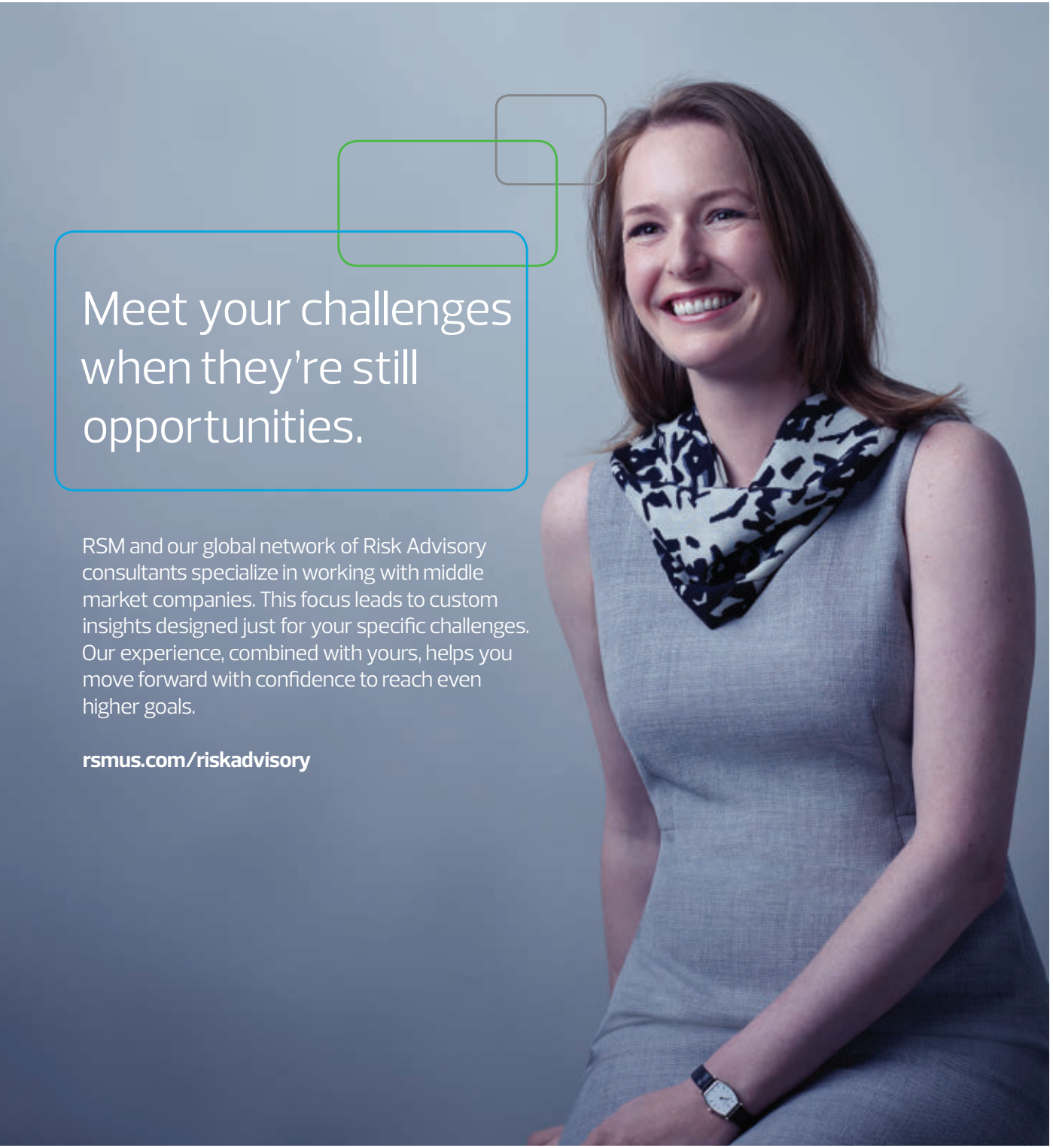
Blowing the Whistle  
on Corruption

An Innovative Audit Internship



## SMALL BUT SAVVY

Audit functions of limited size  
work to get the most out of their technology,  
providing maximum value to stakeholders.



Meet your challenges  
when they're still  
opportunities.

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

[rsmus.com/riskadvisory](https://rsmus.com/riskadvisory)

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



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





# A transforming moment for internal audit

**Technology and an ever-accelerating pace of change present internal audit groups with unprecedented challenges.**

These challenges present internal audit teams the opportunity to transform their place in the organization. The transformation journey begins with a solid road map to reimagine, validate, mobilize, and execute. To learn more, visit [crowe.com/iatransform](http://crowe.com/iatransform).



**Audit / Tax / Advisory / Risk / Performance**

**[crowe.com/iatransform](http://crowe.com/iatransform)**



## Updated – Aligned – Focused

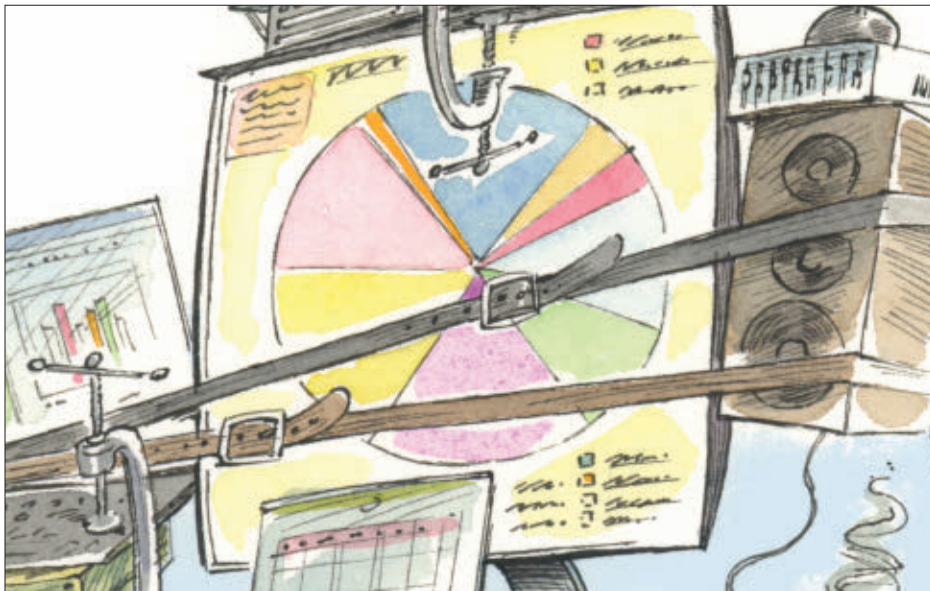
As the only globally recognized certification for internal audit, the Certified Internal Auditor® (CIA®) is changing. If you've been putting off earning your CIA, it's time to take a fresh look at this important step toward validating your knowledge, skills, and ability to carry out professional responsibilities for any audit, anywhere.

---

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







## F E A T U R E S

**24 COVER Small But Tech Savvy** Audit functions with limited resources are maximizing stakeholder value by making the most of their technology. **BY ARTHUR PIPER**

**31 6 Steps to Right-size Internal Audit** With the right benchmarking measures, CAEs can effectively size their internal audit departments. **BY STEPHEN SHELTON**

**36 The Rise of Automation** Emerging technologies such as AI present a host of risks, and opportunities, for auditors to consider. **BY MICHAEL ROSE, ETHAN ROJHANI, AND VIVEK RODRIGUES**

**43 Penalizing Corruption** The U.S. SEC's Whistleblower Program has fined companies

more than \$1 billion since 2011. **BY DANIEL GAYDON AND DOUGLAS M. BOYLE**

**51 Breaking Free of Mental Traps** Internal auditors can take steps to avoid overthinking that can impact audits and service to clients. **BY MURRAY D. WOLFE**

**56 Real-world Education** A university and health-care company partnered to create an internal audit internship program that equips students to hit the ground running. **BY RINA M. HIRSCH**



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

# Deloitte.



## The innovation imperative

Forging internal audit's path  
to the future

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

Learn more at [www.deloitte.com/globalcaesurvey](http://www.deloitte.com/globalcaesurvey)

## DEPARTMENTS



**7 Editor's Note**

**8 Reader Forum**

**67 Calendar**

### PRACTICES

**10 Update** Leaders missing the mark on strategic threats; digital initiatives rise to boards' agenda; and directors focused on what they know.

**14 Back to Basics** Aligning R&R audits with objectives.

**17 ITAudit** Blockchain's challenges and opportunities.

**20 Risk Watch** Auditors should assess oversight of transformative projects.

**22 Fraud Findings** A controller steals \$4 million to fund a new business venture.

### INSIGHTS

**60 Governance Perspectives** Launching a small audit function takes patience and focus.

**63 The Mind of Jacka** Few organizations will pay a premium for internal audit.

**64 Eye on Business** Boards are taking a closer look at culture.

**68 In My Opinion** Auditors should contribute to the collective public good.

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



### Crimes of the Century

*Internal Auditor* takes a look back at some of the most infamous corporate frauds of the 21st century.

### Small But Significant

Watch the CAE at a nonprofit insurance provider explain how technology and unique strategies have helped her small audit function succeed.

**Mining Processes** An addition to the toolkit can give internal auditors a clear picture of business processes.

**An Injection of Fraud** A health-care CEO pleads guilty to scheming to pay physicians for unnecessary treatments. Auditors need to look out for medical fraud disguised as legitimate care.





# 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.**

**Pre-order Today!**\* [www.theiia.org/Sawyers](http://www.theiia.org/Sawyers)

\* Ships early January 2019.

  
INTERNAL AUDIT  
FOUNDATION™





## THE SMART, SMALL INTERNAL AUDIT FUNCTION

**A**t an IIA Audit Executive Center CAE roundtable discussion early this year, some participants shook their heads when asked what it would take to make their audit functions more innovative. Participants said they didn't have the resources to even consider innovating. However, Jim Pelletier, IIA vice president of Professional Standards and Knowledge and InternalAuditor.org's innovation blogger, told them they should not consider lack of resources a roadblock to innovating, as it only takes one person to think differently and challenge the status quo.

Approximately one-fourth of North American IIA members are full-time employees of small (one- to five-person) audit functions, according to The IIA's 2018 Member Needs Survey. In this month's cover story, "Small But Tech Savvy" (page 24), CAEs of small functions discuss how they are using technology creatively, efficiently, and cost effectively. "Through innovative techniques and keen attention to stakeholder needs, many small audit functions are making the most of the technology tools at their disposal," author Arthur Piper writes.

Innovation and flexibility go hand in hand. "With limited resources comes limited time, but small audit functions must maintain flexibility when events occur that are outside the scope of the audit plan," writes Justin Stroud, who was brought in as Western Reserve Group's one-person audit department nearly four years ago (see "Governance Perspectives" on page 60). "Having laser focus and a detailed game plan can help squeeze in work that can add value to the organization."

And small audit departments have been known to do great things! In this month's "Fraud Findings" (page 22), read how a lone internal auditor worked with a forensic investigator to uncover a nearly \$4 million embezzlement—no small feat.

So, here's to the small but mighty audit function, the men and women who work tirelessly to enhance and protect organizational value. These small teams are succeeding through agility and innovation.

A handwritten signature in black ink that reads "Anne".

@AMillage on Twitter

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



## COSO for Technology Implementation

Paul Sobel's article makes The Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management—Integrating With Strategy and Performance* easy to absorb. I agree that this is the framework in which to consider failure risks for IT projects required to implement corporate strategic direction. Corporate strategy execution these days often relies on successful technology implementation. So, this is an internal audit and board-level issue.

**ROBERT MCKEEMAN** comments on Paul Sobel's "In Any Kind of Weather" (October 2018).

## Active Directory vs. HR Database

I found Manoj Satnaliwala's article a decent, high-level discussion on the topic of physical access. However, he made a rather serious misstatement with his reference to Active Directory (AD) as a human resources database. For one, it should have been called Microsoft Active Directory, which would likely have prevented the faux pas. Microsoft Active Directory

is a core technology component of IT infrastructure that Microsoft uses for the management of users, devices, sub-domains, etc., and is considered the Microsoft implementation of Lightweight Directory Access Protocol (LDAP). While organizations use both AD and LDAP to drive logical access control, it is not directly used for physical access controls, unless it is paired with physical access devices that validate against it.

**KARIM MERALI** comments on Manoj Satnaliwala's "Don't Overlook Physical Access" (October 2018).

**Author's Response:** *Thanks for highlighting this oversight. The statement was out of context and should have read, "For example, many organizations use Active Directory to validate an employee's access credentials in real time." The idea was to highlight the integration and automation of the processes and connect to one source for a true Active Directory.*

## Renaming the Profession

I like the idea of internal assurance service, Mike. A few of the departments I work with use global assurance services, but I prefer keeping the word "internal" in the name. Should we open a can of worms and expand our thinking beyond assurance and consider the other roles that internal audit performs for many companies such as compliance, risk management, or quality assurance?

**RAVEN CATLIN** comments on the "From the Mind of Jacka" blog post, "Internal Audit by Any Other Name" ([InternalAuditor.org](http://InternalAuditor.org)).



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



**EDITOR IN CHIEF**  
Anne Millage

**MANAGING EDITOR**  
David Salierno

**ASSOCIATE MANAGING EDITOR**  
Tim McCollum

**SENIOR EDITOR**  
Shannon Steffie

**ART DIRECTION**  
Yacinski Design

**PRODUCTION MANAGER**  
Gretchen Gorfine

### CONTRIBUTING EDITORS

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

### EDITORIAL ADVISORY BOARD

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

Jorge Gonzalez, CIA, CISA  
Nancy Haig, CIA, CFE, CCSA, CRMA  
Daniel Helming, CIA, CPA  
Karin L. Hill, CIA, CGAP, CRMA  
J. Michael Jacka, CIA, CPCI, CFE, CPA  
Sandra Kasahara, CIA, CPA  
Michael Levy, CIA, CRMA, CISA, CISSP  
Merek Lipson, CIA  
Thomas Luccock, CIA, CPA  
Michael Marinaccio, CIA  
Alyssa G. Martin, CPA  
Dennis McGuffie, CPA  
Stephen Minder, CIA  
Jack Murray, Jr., CIA, CRP  
Hans Nieuwlands, CIA, RA, CCSA, CGAP  
Manish Pathak, CA  
Bryant Richards, CIA, CRMA  
Jeffrey Ridley, CIA, FCIS, FIIA  
Marshall Romney, PHD, CPA, CFE  
James Roth, PHD, CIA, CCSA  
Katherine Shamai, CIA, CA, CFE, CRMA  
Debra Shelton, CIA, CRMA  
Laura Soileau, CIA, CRMA  
Jerry Strawser, PHD, CPA  
Glenn Summers, PHD, CIA, CPA, CRMA

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

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

**IIA CHAIRMAN OF THE BOARD**  
Naohiro Mourf, CIA, CPA



**PUBLISHED BY THE  
INSTITUTE OF INTERNAL  
AUDITORS INC.**

### CONTACT INFORMATION

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

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

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

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

**WRITER'S GUIDELINES**  
[InternalAuditor.org](http://InternalAuditor.org) (click on "Writer's Guidelines")

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



---

# 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://InternalAuditor.org).

**Ia**  
INTERNAL AUDITOR

Nations' money-laundering risks rise... Directors lack innovation focus... Adopting emerging technology... Boards unprepared for digital challenges.

# Update



Chief audit executives are highly confident in internal audit's ability to provide assurance in five risk areas.

- ✓ **58%**  
Data privacy
- ✓ **55%**  
Third parties
- ✓ **53%**  
Cybersecurity
- ✓ **51%**  
Data governance
- ✓ **45%**  
Culture

Source: Gartner, 2019 Audit Plan Hot Spots Report



## MISSING THE MARK ON STRATEGIC THREATS

Almost all CEO (95 percent) and board member (97 percent) respondents to a recent survey expect their organizations will face serious threats or disruptions to growth in the next two to three years. Yet, Deloitte's Illuminating a Path Forward on Strategic Risk survey reports that many are not effectively prioritizing the strategic planning and investing needed to address critical risks.

"Leaders know there are threats on the horizon, but many are not viewing or managing them strategically or understanding

Many CEOs and board members are underestimating reputation and culture risks in their organizations.

how threats are interconnected," explains Chuck Saia, CEO of Deloitte Risk and Financial Advisory.

Deloitte surveyed 400 CEOs and board members from U.S. organizations with \$1 billion or more in annual revenue about brand and reputation, culture, cyber risk and technology, and the extended enterprise. Respondents say the greatest threats to growth are new disruptive technologies, cyber incidents, extended enterprise/third parties, erosion of brand reputation, and weak organizational culture.

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

IMAGES: TOP, T. DALLAS / SHUTTERSTOCK.COM; LEFT, T. VECTOR-ICONS / SHUTTERSTOCK.COM



The report notes that CEOs and boards are focusing on digital transformation and disruptive technologies. However, they aren't as concerned about protecting their brand and reputation. Only half of board members and 42 percent of CEOs have discussed reputational risk in the last year.

To help determine an organization's strategic risk preparedness, organizations should ask questions such as: Is management receiving the information it needs to understand and address strategic risk? What steps are being taken to proactively address these risks? — **S. STEFFEE**

## CORRUPTION RISK RUNS HIGH WORLDWIDE

**G**overnance index shows increased vulnerability to money laundering.

**M**ost countries are making little progress toward ending corruption, according to the Basel Institute on Governance's annual assessment of money-laundering risk.

The 2018 Basel Anti-Money Laundering (AML) Index rated nearly two-thirds of the 129 countries as having a significant risk of money laundering and terrorist financing.

Higher scores on the index, based on a 10-point scale, indicate greater vulnerability. More than 40 percent of countries received higher scores compared to 2017.

Failure to implement AML measures is at least partly to blame for the worsening scores, according to the institute. "Governments may be ticking the right boxes in



terms of formal compliance, but in reality neglecting enforcement of laws and measures to prevent and combat money laundering and related financial crimes," says Gretta Fenner, managing director at the Basel Institute of Governance.

Low-risk countries share several characteristics, including comprehensive measures for domestic and international cooperation, high levels of press freedom, and high levels of transparency and integrity. — **D. SALIERNO**



**37%**  
**OF BUSINESS EXECUTIVES AT SMALL AND MID-SIZED COMPANIES** say their organization received an email requesting payment from someone pretending to be a senior manager or vendor.

**47%**  
**SAY EMPLOYEES RECEIVING SUCH EMAIL RESPONDED BY TRANSFERRING COMPANY FUNDS.**

"Even companies that have information security training and fairly savvy employees fall victim to these deceptions," says Timothy Zeilman, vice president of The Hartford Steam Boiler Inspection and Insurance Co. (HSB).

Source: Zogby Analytics for HSB

## INNOVATION CHALLENGED

**D**irectors may not be prepared to address unfamiliar risks.

**I**n an age of disruptive innovation, boards are paying more attention to what they know, a Harvard Business School survey reports. According to the *Harvard Business Review*, less

than one-third of more than 5,000 board members polled say innovation is a top-three organizational challenge.

Indeed, innovation ranks fifth in the global survey, behind finding top talent, the

regulatory environment, and global and domestic competitive threats. The problem may be that innovation and technology are not directors' strong suits. Only 42 percent rate their board above average or excellent in these areas.

Nor are boards likely to focus more on innovation

soon. Just 13 percent say they prioritize technology expertise when recruiting new directors.

Even so, researchers J. Yo-Jud Cheng and Boris Groysberg say an innovation focus and board performance are correlated. “The boards with strong innovation processes tend to be the ones that are performing well on all fronts,” they say.

Directors’ focus on what they know may impede their ability to oversee today’s disruptive risks. That’s because boards tend to focus more on known risks than on risks that could have a significant, severe, and often sudden effect on the organization, notes a report from the National Association of Corporate Directors’ (NACD’s) Blue Ribbon Commission on Adaptive Governance.

“Disruptive risks won’t wait for boards and management teams to catch up,” says commission co-chair Sue Cole. “Put simply, these forces have the ability to make or break an organization’s success.”

To strengthen oversight, the report recommends boards improve the content and format of reports on disruptive risks from management and seek information from outside sources. Moreover, it advises boards to stay informed about the company and its industry, as well as have deep discussions with management about how disruptive risks could impact the organization’s strategy. — **T. MCCOLLUM**

## DRIVING TECHNOLOGY ADOPTION

Asif Siddique, head of Global Technology & Privacy Assessments at Oracle Corp., says internal audit has a role to play in emerging technologies.



**How can internal audit contribute to the adoption of transformative technologies, such as artificial intelligence and machine learning?** As with all emerging technologies, internal audit should be on the forefront, working with the business to understand key risks and how the company plans to use them, and ensuring they are appropriately evaluated during risk and project planning. When we identify issues during the audit process, the related action plans/recommendations can be tailored to encourage the use of these technologies.

These technologies provide internal audit with smart tools to capture risks differently. Because our audits involve a growing list of products containing these technologies, they impact our talent model. They are changing the way we plan audits and forcing us to reevaluate our resource model and deployment. It also provides an opportunity to perform advanced analytics to get relevant samples based on the emerging privacy and security landscape globally. If select testing can be automated using machine learning and artificial intelligence, internal audit can leverage available resources to cover additional areas and provide deeper insight into the effectiveness of technology controls. And enterprisewide trends and anomalies can be identified and researched more efficiently.

## BOARDS WEIGH IN ON DIGITAL INITIATIVES

Many organizations aren’t prepared for cyber challenges.

No longer strictly the domain of IT, digital strategy has risen to the top of board agendas, according to a recent survey by accounting and advisory firm BDO USA. Nonetheless, many organizations remain unprepared for cyber risk and other digital challenges.

BDO’s 2018 Cyber Governance Survey, which polled nearly 150 board directors from publicly listed U.S. companies, indicates that nearly half of companies have increased spending on digital initiatives and 29 percent have hired board members with relevant oversight skills. Moreover, two-thirds of respondents say their company has a digital transformation strategy or is developing one.

Still, the remaining one-third of respondents’ companies have not put a



transformation strategy in place — nor do they foresee developing one in the near future. And while 72 percent of directors say they are more involved with cybersecurity now compared to 12 months ago, more than 20 percent admit their organization has not implemented an incident response plan. — **D. SALIERNO**





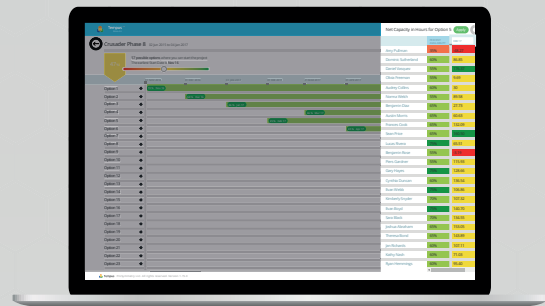
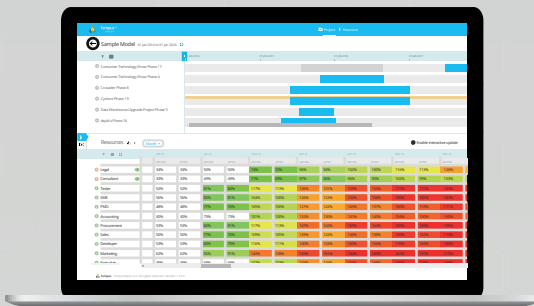
# Tempus Resource

A Gartner 2016 PPM Cool Vendor  
for Resource Planning



“ProSymmetry provides a  
Resource Management Solution  
accessible to the masses.”

Robert Handler  
VP Distinguished Analyst, Gartner



Find your replacement for spreadsheets.  
Resource modelling capabilities give  
you instant visibility over project  
changes as they happen.

Tempus Resource also provides  
advanced scenario planning through  
temperature mapping to better  
visualize your resource allocation.



(+1) 713 - 985 - 9997



[prosymmetry.com](http://prosymmetry.com)



[info@prosymmetry.com](mailto:info@prosymmetry.com)

# Back to Basics

BY SHILPA YADAV    EDITED BY JAMES ROTH + WADE CASSELS

## ADDING VALUE IN R&R AUDITS

Internal auditors can focus on specific areas of revenue and receivables audits to ensure alignment with organizational objectives.

With an organization's internal controls being tested more than once a year via external auditors and regulatory requirements, such as the U.S. Sarbanes-Oxley Act of 2002, what additional value does an internal auditor bring? Internal auditors can look beyond the financial statement's accuracy and focus on control reviews to ensure its alignment with management's objectives and strategies—specifically in the revenue and receivables process.

External auditors and in-house Sarbanes-Oxley auditors perform test procedures to validate various assertions related to revenue transactions, receivables balances, and their presentation and disclosures in the financial statements. Internal auditors can work with management to ensure that the revenue and receivables processes are set up and controlled effectively to achieve

the organization's goals. There are several areas on which internal audit can focus to help achieve this objective.

### Pricing Strategy

Internal auditors should interview senior management to get insight over the assumptions, historical sales growth analysis, customers' feedback and forecasts, and other resources tapped to gain the pulse of the market. This insight will help internal auditors assess if the pricing strategy is moving in the right direction to help the organization achieve its goals. If not, internal audit should discuss with management how to improve the analysis and pricing strategy.

Once satisfied with the pricing strategy, internal auditors should then evaluate transformation of this strategy into the actual pricing structure, assess whether the framework provided to the sales team for negotiating with customers aligns with the pricing strategy, and

ensure that the approvals for pricing structure and negotiations include exceptions to the pricing strategy.

### Having the Right Customers

In a business-to-business model, working with profitable and creditworthy customers is a sign of sustainability and consistent growth year over year. When reviewing the customer selection process, internal audit should:

- ➔ Check the existence and adequacy of customer selection policies approved by the appropriate level of management.
- ➔ Ensure adherence to these policies.
- ➔ Assess the adequacy and reliability of resources used to check customers' credit rating (good credit provides reasonable assurance over revenue collection).
- ➔ Evaluate profitability at a customer level and

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 [shilpa.yadav@theiia.org](mailto:shilpa.yadav@theiia.org)

question management on loss-making deals (profitability analysis provides visibility over profitable deals).

- ➔ Review the effectiveness of controls over updating customer data in the organization's customer database to ensure data validity.

### Contractual Obligations

This area is more applicable to organizations that provide a complex bundle of services. Such sales need a well-drafted contract detailing all performance obligations. Internal auditors should check for the existence of a control where contracts are reviewed by legal experts, an accounting policy team, and an operations team, and are approved by the appropriate management level to protect the company from unwanted obligations and commitments.

If a contract template with standard clauses is already developed, the auditor's job is to focus on any nonstandard terms agreed upon by customers and assess their reasonability and approval process effectiveness. Internal audit should risk-rank the contracts based on their contribution to the organization's objectives and then develop a testing strategy to review the reasonableness of key nonstandard terms. The higher the number of nonstandard terms, the greater the challenge for internal auditors.

### Conversion of Orders to Invoices

Internal auditors should confirm that a process exists to capture the goods or services provided to customers and

**Internal auditors should analyze write-off data to identify outliers.**

to invoice them for these goods or services. Prices for goods and services sold by the organization should be updated in the price database, and the revenue system must capture all goods and services sold to customers for accurate invoicing.

Usually, internal auditors test these processes on a sample basis. To make the sample selection effective, internal auditors should pick up on clues about process gaps, control weaknesses, and system constraints through process map reviews, data analytics, rework queues, pain points, and process improvement ideas communicated by management. These areas could reveal missing management oversight and potential revenue leakages, such as not invoicing for services provided or generating invoices with lower-than-negotiated rates.

### Tracking Receivables and Collection Efforts

The receivables aging report is a good source to determine tracking process efficiency. External auditors and Sarbanes-Oxley auditors review the aging report for valuation and to reconcile with the financial statements, while internal auditors can assess the effectiveness of its collection efforts. Does follow-up with customers happen with sufficient frequency and is there a process to escalate problematic dues with senior management? Also, are the receivables that are handed over to collection agencies, either under litigation or from bankrupt customers, being tracked to protect the company's interests?

Although write-off approvals are reviewed by external auditors and Sarbanes-Oxley auditors, internal auditors should analyze write-off data to identify outliers, such as the same employee writing off certain customers' dues frequently or the same customers' dues getting written off often. The root causes of these outliers will help reveal the process control issues.


### Recording Cash Receipts

Recording cash receipts is vulnerable to misappropriation of cash received from customers and is reviewed by external auditors and Sarbanes-Oxley auditors. Cash receipts include electronic fund transfers, checks, credit cards, and physical cash receipts. Internal auditors can focus on the timeliness of recording the collection of cash in addition to the adequacy of segregation of duties and sufficient oversight in receiving, depositing, and recording cash funds.

### Performance Metrics

Last but not least are the metrics developed by management to measure the performance of revenue and receivables processes. Internal audit should review the accuracy of key metrics to ensure that the data used for metrics calculations are correct and current. Internal auditors also can suggest additional metrics that will be useful to management.

### Focus on What Matters

By reviewing end-to-end processes and questioning the alignment of various policies, procedures, and performance metrics with management's corporate objectives, internal audit can enhance the work of external and Sarbanes-Oxley auditors. Working with management to finalize the objective and scope of audits will help auditors focus on the risks that really matter to management, in addition to reviewing key internal controls that matter to internal auditors. 

**SHILPA YADAV, CPA, CGA, CA (India)**, is a senior internal auditor for Canadian Pacific Railway in Calgary.



## **Audit Management Software**

✓ **No Gimmicks**

✓ **No Metaphors**

✓ **No Ridiculous Claims**

✓ **No Clichés**

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

**Just Brilliant Software.**

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

*Trusted by Companies, Governments and Individuals Worldwide.*

## AUDITING BLOCKCHAIN

Internal auditors need to focus on new risks and opportunities posed by blockchain technologies.

**B**usinesses and government agencies alike are pursuing blockchain's promise of greater accuracy, transparency, and efficiency. Accounting firms are investing more than \$3 billion a year on blockchain technology, while IBM predicts that two-thirds of all banks will have blockchain products by 2020. These organizations are attracted to blockchain's ability to record relevant details of every transaction in a distributed network.

Like other new technologies, blockchain presents challenges and opportunities for internal auditors. Blockchain carries the typical IT risks such as unauthorized access and threats to confidentiality, but it also could impact traditional audit procedures. Yet, blockchain may enable auditors to be more innovative and efficient.

### The New Risks

As with all new technologies, internal auditors need

to assess the internal and external risks to business objectives posed by blockchain. One risk is a "51 percent," or "majority rule," attack. In this attack, a user introduces false data in the blocks to create a fraudulent transaction that most nodes on the blockchain accept as true. Hackers also could target endpoint vulnerabilities where people interact with the blockchain, which is when the data is most susceptible to attack.

Another risk is individuals in a supply chain who misuse data by manipulating a blockchain's transparency and traceability features. Legal risks arise from the lack of standards and regulations for monitoring blockchains in diverse legal jurisdictions worldwide.

Against this backdrop, internal auditors should review whether their clients have established appropriate actions to mitigate risks, including the timelines and staff needed to deploy them.

Auditors also should provide assurance on the risks associated with implementing blockchain such as technology interfaces with legacy systems and the adequacy of migration strategies.

### Testing Systems

Unlike traditional databases, blockchain applications maintain data in blocks, also known as a distributed ledger. These blocks are accessible to all users who are permitted to access them. Because a blockchain does not have a master copy of the database controlled by a database administrator, there is no single point of failure in the event of hacking. Instead, the ledger is replicated in many identical databases, each hosted by a different party. Any change carried out in one copy will simultaneously change all the records.

Notwithstanding blockchain's security features, internal auditors should ask these questions while testing the system:

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





## Get all the tools and resources to audit more effectively.

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

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

Standards Practice Makes Sense  
[www.theiia.org/HaveStandards](http://www.theiia.org/HaveStandards)

 **The Institute of  
Internal Auditors**



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

- ➔ How does blockchain allow different parties with distributed responsibilities in the network to access the ledgers when there is no central administrator?
- ➔ How fast and timely is data available as millions of transactions are written simultaneously? Were availability risks addressed at the design stage?
- ➔ How safe are the authorizations that allow users to read and write in the blocks? Are these confidentiality risks?
- ➔ How adequate are the cryptography arrangements in place to hide the database in the network to ensure completeness, integrity, and nonrepudiation of data?
- ➔ How robust are the validation controls and the roles allocated in view of limitations on reversing the transactions? Once blocks in a chain are secured through hashing, they cannot be reversed.
- ➔ How adequate are the arrangements over the audit trail when there is no centralized database?
- ➔ How adequate are the controls over the data backup and disaster recovery processes considering there are multiple copies of the blockchain and no single point of failure? Also, what arrangements are in place to recognize the node/ledger that could be used for backups?

### Impact on Procedures

Blockchain has implications for financial statement audit procedures. Because data maintained in blockchains is available in real time, traditional sampling techniques used in financial statements may not be required. Internal auditors can provide assurance by using data analytics to scan the entire database. Additionally, conventional reconciliation and validating tasks

## Blockchain may render many risks related to financial statements obsolete.

may not be necessary because there should not be discrepancies in the financial statements in a shared ledger scenario.

Indeed, blockchain may render many current risks related to financial statement opinions obsolete. Auditors should be aware of the new risks and their impact on traditional audit procedures.

One example is the risk of auditing transactions captured in an immutable blockchain. During a financial audit in a blockchain environment, auditors will be able to assess whether the transactions recognized in the financial statements have occurred and relate to the entity. However, in doing so, they might overlook the audit evidence's relevance, reliability, objectivity, and verifiability. This is because auditors could

treat the acceptance of a transaction into a reliable blockchain as sufficient audit evidence. Likewise, blockchain might legitimize certain off-ledger transactions or incorrectly classify the transactions, providing false assurance.

Blockchain may require internal auditors to allocate more resources to obtain assurance on the adequacy of controls in recording transactions. Moreover, auditors will continue to focus on issues related to other nonautomated key activities such as governance, risk management, monitoring, reporting, and evaluation. Indeed, value-for-money audits and other types of audits may grow as organizations seek to evaluate the costs and benefits associated with blockchain applications.


### Opportunities for Audit

Blockchain may not completely redefine the rules of internal auditing, but it could provide new opportunities. First, auditors could lobby their clients to involve them during system development either as observers or advisors. This would help auditors understand the nuances of the blockchain operating environment from its inception, including its implementation challenges. Moreover, auditors may be able to suggest and determine the terms of reference for developing appropriate audit modules in blockchain-based systems.

Second, blockchain may encourage audit management to streamline and reorient its staff, while building the department's capacity to provide quality services to clients. Staff members will need to be able to work with a range of new technologies. Conversely, by automating some tasks, internal audit functions may not need as many auditors as before.

Third, artificial intelligence may enable auditors to quickly process, extract, and identify risks up front using publicly available blockchain ledgers. This ability may make the audits more cost-effective. Also, auditors could use data mining to identify the highest risks such as frauds, resulting in more relevant audits.

### Built to Thrive

As blockchain changes the way business is conducted globally, it presents an opportunity for internal auditors to migrate to a challenging, new operating environment. To get there, internal audit must evolve its procedures while staying focused on the risks that matter most to the organization. By monitoring blockchain developments, auditors can help the business thrive in the future. 

**ISRAEL SADU, PHD, CIA, CRMA, CISA**, is resident auditor with the United Nations Office of Internal Oversight Services in Bonn, Germany.

# Risk Watch

BY ASHOK (ASH) KANNAN

EDITED BY CHARLIE WRIGHT

## A NEW AGE OF IT GOVERNANCE RISK

Internal auditors need to plan for assessing oversight of transformative technology projects.

**E**ffective governance of IT is critical to organizational success and can transform an organization. While IT-enabled transformation can bring many rewards, poor governance of those projects can cause disruption and unintended consequences.

As an organization evaluates different technology investments, management must ensure the technology is aligned and delivered in accordance with the organization's strategies and objectives. Internal auditors can help by providing independent assurance on the appropriateness and effectiveness of the governance structure.

### Technology's Challenge

IT departments manage the technology supporting business applications, disaster recovery, cloud services, and other mission-critical functions. In many organizations, the IT infrastructure is the foundation for business operations. Yet,

new technology often creates new risks ranging from specific control weaknesses to potentially enterprise-wide disruptions. Helping the organization assess and address these risks is an opportunity for internal auditors to add value.

According to Standard 2110-A2 of the *International Standards for the Professional Practice of Internal Auditing*, internal audit must assess whether IT governance supports the organization's strategies and objectives. Consequently, the challenge for internal auditors is to help assess numerous risks associated with governance of enterprise IT.

### Frameworks

Audit programs will be more useful if they differentiate governance risks from risks related to the management of enterprise IT. Internal auditors can leverage a variety of frameworks to develop high-quality, tailored audit programs for IT governance.

Governance frameworks include The Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control—Integrated Framework*, ISACA's COBIT, and the Balanced Scorecard Institute's Balanced Scorecard. Organizations also can use management frameworks such as ITIL, the U.S. National Institute of Science and Technology's Cybersecurity Framework, and the International Organization for Standardization's ISO/IEC 27001: Information Security Management, ISO/IEC 38500: Information Technology—Governance of IT, and ISO 9000: Quality Management. These frameworks explain risks, controls, and other details that can reduce the time required to develop an audit program.

### Audit Planning

Internal auditors should become familiar with each of the governance frameworks so they can scope the audit engagement to focus

SEND RISK WATCH ARTICLE IDEAS to Charlie Wright at [cwright@bkd.com](mailto:cwright@bkd.com)





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

on the appropriate risks. Audit programs should identify the impact of IT risk to the organization as well as the potential for compliance failure. During the risk assessment, auditors can determine the current state of risk management practices, assess design gaps, identify improvement opportunities, and recommend actions. They should consider several areas in their audit program.

**Strategic Alignment** IT strategic alignment continues to be a top priority for most organizations and aligning technology with business strategies can be challenging for management. One of the key governance controls auditors can review is the process and methodology for justifying and prioritizing IT investments. Auditors can verify that the organization has a formal and periodic process for identifying business needs. Audit procedures also should validate that the IT budget cycle is part of the business operations budgeting process. Additionally, auditors can validate corporate objectives and strategic goal alignment by reviewing the decision rights and accountability framework documentation.

**Roles and Responsibilities** IT executives need to collaborate with business-unit executives to ensure technology helps shape business strategy. Without clearly defined roles and responsibilities for IT management, the organization might risk not aligning IT and enterprise operations. To identify the links between business and IT plans, internal auditors can evaluate the strategic plan for IT-enabled initiatives, policies, presentations to the board that highlight the outcomes of a successful implementation, and third-party agreements. Additionally, auditors should verify IT's involvement and responsibilities in the sourcing process. Appropriate involvement by IT can ensure new technology fits the organization's current environment. Additionally, auditors, IT, and the information security group can collaborate to evaluate compliance requirements.

**Organizational Structure** To enable better governance, the chief information officer should be part of an executive or senior management team and an active participant in setting business-unit-level strategy and goals. With the pace of change in today's business environment, the IT organization must be agile and responsive, so auditors should review metrics associated with the length of projects as well as service satisfaction.

Auditors should try to identify unauthorized IT projects by business units—known as shadow IT—by reviewing technology acquisition processes, purchasing authority, application inventory, and sourcing processes. They should work with the IT support function to evaluate internet traffic to external sites that may identify unauthorized subscriptions to software as a service applications. Based on a sample, auditors


can review IT's level of participation on the organization's steering committees and internal advisory boards.

**Risk Management** Auditors should evaluate whether IT risks are included in the enterprise risk management program. Auditors also can review internal processes that identify, communicate, and manage IT risks. Change controls are a huge risk in this area, so auditors should review risk management activities such as communications planning, change management, and committee oversight. If the organization has a security operations center, auditors should assess how it manages the IT environment and responds to incidents.

**Project Management** Organizations should have a project management office to provide governance to prioritize IT projects according to business need. Auditors should review program and project management methodology and ensure the organization complies with internal processes to request, evaluate, and approve IT projects. They should examine a sample of completed projects to determine whether those initiatives realized stated benefits. Moreover, auditors should review the process for evaluating and prioritizing projects at the business-unit and enterprisewide levels. Additionally, understanding and reviewing key performance metrics, such as planned vs. actual expenses and requirement backlog would be invaluable.

**Management Activities** Without an appropriate focus on technology, organizations could mismanage critical IT resources such as the application environment, data, infrastructure, and people. Auditors should evaluate IT's involvement in key projects, the demand forecasting process, and resource management practices. IT's involvement and assessment before engaging software providers and consultants will help mitigate the implementation risks associated with large projects. Robust demand and resource management practices can provide the bottom-up approach to gain insights into business requirements, alignment, and priorities. By understanding IT resource commitments, internal audit can assess the organization's ability to deliver on key initiatives.

### Identifying Key Risks

Every organization's risk profile is unique and depends on the organization's culture, structure, and mission. Governance and management teams should identify and prioritize key risks for mitigation and formalize risk acceptance. Organizations should leverage internal audit's knowledge of the business' environment, IT investments, and internal processes. 

**ASHOK (ASH) KANNAN, CISA, CISSP**, is a senior audit professional at Devon Energy in Oklahoma City.

# Fraud Findings

BY FRANK RUDEWICZ + ERICA HEINZ    EDITED BY BRYANT RICHARDS

## A CASE OF MISPLACED TRUST

A long-time company employee steals \$4 million to fund her business venture.

Jane Dosh was the comptroller and a trusted employee at Smith Interior Design Co. (SID), a small and close-knit professional services firm catering to high net-worth families and individuals, for almost 15 years. As comptroller, she managed many aspects of SID's financials—such as paying bills, managing payroll, and purchasing supplies for the company and clients—with oversight from Robert Smith, the company's co-founder. Smith was responsible for monitoring the company's finances. When he passed away in 2011, his financial responsibilities were added to Dosh's workload, which meant she handled every aspect of the company's finances with no oversight. She continued in that role for the next few years until she unexpectedly resigned on Dec. 31, 2016.

Internal Audit Manager Heather Dittman was the sole internal auditor at

SID and did not have the resources to provide a routine set of reviews aligned with a regular risk assessment. As part of her annual plan, Dittman performed a standard review of the accounts payable process. The audit program included sampling transactions, checking support, and ensuring appropriate authorizations. During her review in early 2017, she documented several unsupported and unexplained transactions.

During the validation process, Dittman interviewed several employees for supporting explanations and documents, but they were unaware of the expenses and could not retrieve the records. Having exceptions in the validation process was a typical event for Dittman, but a large number of unexplained exceptions was unusual—plus there was no supporting documentation.

Dittman reached out to Dosh, who insisted that the records must be misplaced

and that she would find them and send them to Dittman. However, as days turned into weeks, Dosh did not send the records. Dittman sent numerous follow-up emails and voicemails, which went unanswered. After weeks of no response, Dittman went to the file room to search for the records, herself, but the room was empty.

Unable to obtain answers from Dosh and concerned about missing records, Dittman escalated her concerns to the CEO and chief financial officer and recommended a forensic review. Given Dosh's control of the financial processes, it appeared possible that she had defrauded the company and was now covering it up. Management was concerned about the extent of the fraud and the company's ability to recoup the money. As a result, management agreed to a forensic review.

The forensic review began with traditional surveillance of Dosh to uncover

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 [frank.rudewicz@theiaa.org](mailto:frank.rudewicz@theiaa.org)

## LESSONS LEARNED

- » No company is immune to fraud. Internal audit needs to help the organization prevent and minimize fraud risks. Small companies that are reluctant to invest the money to provide more internal audit coverage should consider the return on investment in comparison to a \$4 million embezzlement. It is imperative for companies to set up internal policies and procedures that separate duties, promote accurate documentation, and systematically evaluate and counter all potential risk.
- » Internal audit should perform a fraud risk assessment to help leadership in small companies understand the extent of their vulnerability to fraud. Significant procedural or segregation of duties gaps can be identified during the process without requiring substantial investment in audit resources. Many of the control weaknesses in this case would have been uncovered during the assessment process.
- » Internal auditors should include a fraud risk assessment as a standard for their work plans. It applies to every company and is the most compelling method of educating management about fraud vulnerabilities. The act of communicating this tool throughout management is sometimes enough to prevent fraud.
- » Internal audit needs to know when to involve a forensic investigator. Forensic experts can provide different tools, such as recovering erased hard drives and surveillance, and will preserve the chain of evidence in a fraud case.


the facts necessary to figure out the fraud. During lunch on the second day of surveillance, Dosh went to a local boutique. This piece let the investigators assemble the rest of the puzzle.

Dosh wanted to be an entrepreneur, but she lacked funding. When Smith died, another employee, Helen Brown, was granted a company credit card, and Dosh saw her chance. She had access to the new card's information and knew nobody would be monitoring the credit card activity but her. Dosh then contacted Alexandra Johnson, an acquaintance who worked at a luxury clothing store nearby, and the two began a joint business venture. Dosh went to the store where Johnson worked, and they set up a store account using Brown's company credit card. Johnson later quit her job at the boutique and got a job at another clothing store. There, she set up another account with Dosh using Brown's credit card. Dosh also bought expensive jewelry and clothing from other boutiques on the card. She would pay off her purchases on the company card every month from SID's checking accounts.

When forensic investigators recovered the contents of Dosh's company computer hard drive, they found detailed plans for a boutique clothing and accessory business owned by Dosh and Johnson. Private investigators followed Dosh for weeks to locate where she was storing the fraudulent purchases. She also forged the signature of the second company co-founder on multiple fraudulent checks to purchase personal goods and services, including payments to family-owned businesses. Investigators went through years of company financial documents to find that she had embezzled more than \$4 million from the company in just five years.

SID and the investigators turned the case over to federal law enforcement. Dosh pleaded guilty and is awaiting sentencing for charges related to identify theft and fraud. SID implemented several policies and procedures to prevent the company from getting defrauded again, including:

- » Dispersing cash only after appropriate management authorization and only with dual approvals over certain threshold amounts to ensure company funds were being spent for approved business purposes.
- » Reviewing all cash receipts and disbursements as part of a monthly bank reconciliation.
- » Separating financial duties so no one person would handle all of the responsibilities.
- » Backing up all financial transaction source documents to multiple locations so the documents would not be lost if any one location was compromised.
- » Developing a risk assessment program to allow internal audit to review, assess, and identify weaknesses in the internal controls and point out areas of high risk concerning fraud.

SID realized that internal controls do not have to be an impediment that slows down work processes. While there is no such thing as a one-size-fits-all system of internal controls, getting the focus of their internal controls right helped safeguard and develop their business. 

---

**FRANK RUDEWICZ, ESQ., CAMS**, is partner in charge, forensic services, at Marcum LLP in Boston.

**ERICA HEINZ** is a paraprofessional in the forensic services group at Marcum LLP.



# Small but tech



---

# savvy

**Audit functions with limited resources are making the most of their technology.**

**Arthur Piper**

**Illustrations by Gary Hovland**

# T

Technologies such as artificial intelligence (AI) and robotic process automation (RPA) seem a sure way of revolutionizing the value that internal auditors can add to their organizations. But for auditors working in small departments, the budgets to implement such programs are often out of reach.

Does that mean the days of the small audit function are numbered? Will businesses outsource their audit departments to more technologically enabled consultants to enhance returns on their audit investment? Anecdotally, that seems unlikely—the small audit approach is thriving. Its practitioners are vigorous innovators often working within tight budgets. Squeezing every dollar out of their IT programs is critical, so team members use each application to its maximum capacity. There has to be a rock-solid business case for investing both time and money into new audit technologies—and, if there is, audit committees are supportive. Through innovative techniques and keen attention to stakeholder needs, many small audit functions are making the most of the technology tools at their disposal.

## **TAILORED INNOVATION**

“Small audit shops generally innovate within tight constraints,” says Ross Wescott, principal at consultancy Wescott & Associates in Portland, Ore. “They do so by using what they have differently and, if necessary, bringing some new processes to the table. Every new audit innovation should add value to the business while enhancing the audit process itself.”

Wescott says innovation is a mindset that all auditors would do well to adopt—in both small and large teams. Giving themselves permission to innovate is often the biggest step internal auditors need to take—as well as accepting that some initiatives will fail. To be effective, innovation needs to be closely tied to both the needs of the business and to the technological environment the auditor is working in.

“You would perhaps be surprised, but most IT shops and companies are not very technologically advanced—that is, they are not on the leading edge of technological innovation.” Wescott says. “In the majority of companies, IT



“You would perhaps be surprised, but most IT shops and companies are not very technologically advanced.”

Ross Wescott



“You have to build up good relationships and remain independent at the same time.”

Wendy Cooper

lags behind the business’ strategy. The success of an auditor’s IT processes depends on how well they fit their clients’ own infrastructure.”

**BEST FIT**

That does not mean audit functions in all highly digitalized businesses need to adopt the latest technology trends. Wendy Cooper arrived at the U.K. FTSE 250-listed company Sanne Group plc, London, in January as its internal audit director. Sanne Group is investing in internal audit by developing best practices and growing the team from three members to six. But Cooper is not investing heavily in the latest audit technology.

Cooper says Microsoft Office products such as templates in Word and Excel are adequate tools for most small internal audit functions. The former she uses for planning and drafting reports; the latter for the audit team’s risk and control matrix work and for tracking management actions on the team’s recommendations. Having worked at the global Lloyds Banking Group, she has used custom audit tools and understands they can be useful in coordinating the work of dozens of audit teams in multiple locations. But she thinks it is overkill for a small team — not least because it requires hours of audit time to keep them up to date.

In addition to her chosen tools, Cooper uses the business’ IT systems to download data and select samples to be audited. Those systems may be off-the-shelf packages or custom in-house IT systems. Both depend on people within the business helping the audit team.

“You have to build up good relationships and remain independent at the same time,” she says. That can mean audit staff sitting with the IT expert when requesting data and being there when it is collated. The approach has worked well for Cooper,

and she is establishing links with the best people in the business with such IT knowledge.

She expects all internal audit staff members to be able to test IT controls and to be tech savvy. But for specialist reviews, such as on cyber risk, and for auditing complex financial applications, Cooper has built a co-sourcing relationship with a consulting firm. She says that if the need for specific IT audit skills increases, she would consider adding a more specialized IT auditor to the team.

**AUDITING WITH PURPOSE**

David Givans is the one-person audit function at Deschutes County Administration in Bend, Ore. The county’s data is spread across the organization, usually in discreet silos, and like Cooper, he has to work with business managers to access and analyze data from disparate programs. He says auditors in small functions need to have a “very strong charter” to ensure they have the authority to access the data they need.

As county internal auditor, he deals with a wide range of government departments. In 2018, internal audits have included, for example, a health report on the inmates of the county’s jails, a controls audit over \$10 million of revenue from solid waste disposal franchises, and a follow-up report on its recommendations to the Fairs and Expo team at the county.

Givans uses a mix of data mining tools and Excel to perform his audits, but understanding what he wants the technology to do is paramount. “I don’t let the technology drive what I want to do,” he says. “I have a personal passion for data and analysis, and I’ve been pretty resourceful with the data mining tools I have. But it has to be used for a purpose. I want it to help me tell a compelling story in my audit reports.”





VISIT OUR **Mobile App** to see a video on strategies for small audit functions.

He has recently been adding infographics to help him synthesize the data and bolster the arguments that he needs to make. Using such tools is not only an effective way to communicate his findings, but it underlines to the audit committee and to management the benefit those audit technologies provide. In fact, some of the county's departments are keen to use Givans' analytics tools. "That's the perfect outcome," he says.

### KNOWLEDGE AND MATURITY

Auditors need to know their tools inside and out to be able to focus on the questions they want to ask. "The challenge in applying a technology tool is to get to a point where you can do critical thinking with it," Givans says. Training courses are effective for learning the nuts and bolts of specific systems, but often do not address how to use those programs in the auditor's own environment. "A tool can help you ask questions you feel need addressing, but you must understand how it can be used to come up with an answer for your organization," he says.

Using a limited number of audit applications can be a virtue. Taking a deeper dive into existing technologies can prove more effective than adding new software programs, which often have a steep learning curve associated with them, Givans says. "If you have a week's training course on a software package, you need to use that knowledge—otherwise, you will lose it," he adds. Givans aims to apply the tools he has on every audit so they provide maximum value to both the audit function and the administration.

But how do small functions know whether they are keeping pace with how they should be using technology? It is not easy, says Grant Houle, director of audit at the Mohegan Tribe, which owns Mohegan Gaming and Entertainment in Connecticut. Houle's seven-person audit team serves

the central office in the state. He describes the audit tools that it uses as being "well along the maturity scale" because of the continuous resources and commitment the team has dedicated to its model. "You have to put the time and resources into the tools you have chosen to make sure you get



the objectives you defined when you decided to increase your IT capabilities," he says.

The team is heavily involved in using data analytics and the automation of internal audit processes, such as workpapers, time keeping, and risk ranking. As is typical for a smaller function, it has not dipped its toe in the water with more experimental technologies, such as AI. Houle prefers not to. When he meets other audit executives who have invested in such technologies, he often discovers that they are underused if the company has made the financial investment but has underestimated the time commitment to see

it through. Even electronic workpaper solutions, which have been around for decades, will be little more than repositories if the time is not invested in the core process and behavior changes to get value from the technology.

Keeping the team's capability mature is a "work in progress," he says, because the business is expanding rapidly. Mohegan Gaming and Entertainment has centers in Pennsylvania, Washington state, Louisiana, and New Jersey; a second flagship property under development in Seoul, South Korea; and a new development it is adding next year in Niagara, Ontario. Houle assesses the maturity and fitness of any audit capabilities and tools at each of the new properties that comes on board. That can mean either setting up audit from scratch, or enhancing existing tools, if needed. So far, there are three additional auditors based outside of Connecticut in the wider team—but that is likely to grow.

**SECOND-LINE PARTNERSHIPS**

Houle has been innovating his audit capability by finding ways to work with the second line of defense. Although his team has done whole population testing with its analytics software, a key focus that has paid dividends recently is continuous monitoring with automated processes. Under the group's loyalty scheme, players can earn points. On the gaming tables, the way patrons earn these points has a manual side to it—handling playing cards and tracking play for the purposes of earning points. But a lot of data is also collected from real time play, such as from security cameras. The audit team extracts the tracking data files and the scripts they have developed analyzes them for what may be considered red flag incidents on the tables and passes the results of that analysis on to the second line of defense surveillance group. The surveillance team then



  
 The challenge in applying a technology tool is to get to a point where you can do critical thinking with it."

David Givans



  
 Our job is to make sure we focus on the most valuable red flag incidents."

Grant Houle



  
 We have to be professionals who can facilitate change in the organization and not just manipulate data."

Michael Levy

corroborates the red flag incidents with visual evidence to assess whether there has been genuine gaming errors or potential fraud.

"Our job is to make sure we focus on the most valuable red flag incidents, because the surveillance team needs to physically watch the video material in real time for each one—and there may be 200 in a single day," Houle says. He estimates the continuous monitoring software cost as only about 10 percent of the total project budget—the rest is allocated to the time his team has spent in making sure they get the appropriate value from the objectives they have set.

With such a success under his belt, Houle is seeking to take the model his team developed on the gaming tables and to innovate audit processes in other parts of the business. Moreover, like Cooper, he is continually keeping abreast of developments in the organization itself to understand if those systems can be better exploited by the audit team.

"I don't just want to see what is happening on the shop floor," he says. "I want to be plugged in earlier than that—where are we transitioning to the cloud, for instance, and what does that mean for us?" For example, so-called stadium gaming is becoming popular. A physical dealer remains present, but up to 70 people can play the game and place bets via live video links to the internet. Houle says the process is less risky for the casino because, for example, the risk of marking cards or stealing chips is minimal. On the other hand, IT security risks may increase. Houle makes sure he is at those early meetings to understand the new processes and how his team may be able to help.

**BUSINESS CULTURE**

Michael Levy is the director of internal audit for Student Transportation in Wall, N.J., a multinational school bus contractor. While keeping a close eye

37% of organizations worldwide have deployed artificial intelligence or are planning to in the near future, according to chief information officers polled for the 2019 Gartner CIO Agenda survey.

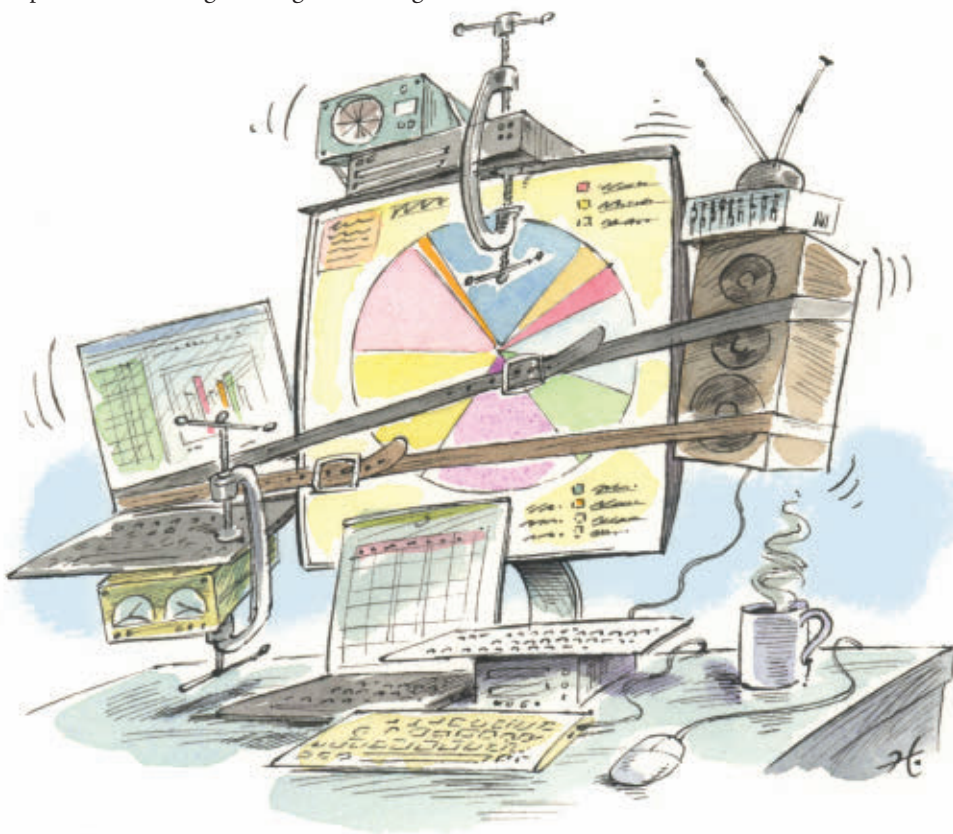
on changing processes at his company, his team of five uses a variety of tools including data analytics, visualization, project management tools, cloud document repositories, and collaboration tools. “It is great to have the ability to use data visualization and analytics, but we as a profession need to make sure we are speaking to our audience and using their language,” he says. “Depending on the project, it sometimes can be better to have those tools used in the background—otherwise you can alienate people.” In addition, he says audit teams need to consider organizational maturity levels to ensure that they do not too far exceed the cultural norms of their organizations. “If we get too far ahead, that could be perceived as a negative,” he says. “We want to be sure as auditors that we do not head down a path that the organization will not perceive value from.”

Although he expects all team members to be conversant with data analytics—someone should be the champion—Levy says that interpersonal skills are also critical for success. “To be successful, we have to be professionals who can facilitate change in the organization and not just manipulate data,” he explains. “That requires relationship building and social skills.” Daily interaction with management helps his team members keep their fingers on the pulse of the organization and be proactive in delivering meaningful change, which data analytics can often help do.

He says he values the efficiencies that the effective use of audit technologies can bring. Automating workpapers, for example, and the process for sending out audit requests has saved his team many hours. However, when he is attending conferences and networking events, he is on a constant lookout for how to use both new and existing tools more intelligently and strategically.

### PRACTICAL TOOLS

As technologies such as AI and RPA become mainstream, small audit functions will most likely use them where the business case is strongest. Audit committees and management are likely to support those efforts because returns will be demonstrable. As Levy notes: “There is no point in over-engineering something



that doesn't need it. That being said, if we can make recommendations to automate business processes, or parts of the audit, that is an intelligent and efficient way of using our resources.” There are lessons for all on how small functions maximize the return on investment from audit technologies. [la](#)

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





Wolters Kluwer

## Small Audit Shops Need to Leverage Technology More than Anyone

Wolters Kluwer TeamMate streamlines the audit process for more than a thousand small audit departments with ten or fewer staff auditors. Small departments face the same challenges as large audit shops, but with fewer resources. Leveraging powerful audit tools can provide you with the efficiency, organization, and quality assurance you need.

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



# STEPS

## to right-size internal audit

With the right benchmarking measures, chief audit executives can effectively size their internal audit departments.

**Stephen Shelton**

**A**t some point in almost every chief audit executive's (CAE's) career, he or she is asked to assess and justify the organization's level of internal audit resources. The number of variables and organization-specific considerations can make this a formidable task because there is no rule or standard to determine the appropriate amount of audit spending. Because judgment and subjectivity are required, CAEs run the risk of being seen as self-serving if the benchmarking exercise is used to advocate increased head count or spending, or to resist internal audit budget reductions in conjunction with broader cost-cutting initiatives.

Considerable judgment is left to the CAE to ensure the audit plan covers the appropriate level of risk. In actual practice, audit committees frequently ask CAEs whether internal audit is sufficiently staffed with respect to number of people and skill. The starting point then, to facilitate "right-sizing" the internal audit function, is to clearly establish and understand internal audit responsibilities, scope, and coverage, as well as stakeholder expectations. To aid this assessment, internal auditors can follow a six-step benchmarking approach

aimed at answering the age-old question: How much is enough?

### **STEP 1** Establish the Purpose for Benchmarking

When internal audit is asked to rationalize budget and head count, stakeholders should consider the current state of the organization and its risk appetite. During times of economic stress, some organizations may be tempted to reduce centralized overhead functions and the corresponding semi-independent oversight of risk, internal control, and business processes. Downsizing also may eliminate administrative and control processes, increase workload, and curtail oversight functions while expanding autonomy and levels of authority. Unfortunately, intense revenue pressure and cost cutting can heighten the risk of inappropriate behavior and shortcuts in controls and business processes.

**Benchmarking should encompass the resources required to meet stakeholder and regulatory expectations.**

Consequently, right-sizing internal audit should go beyond arbitrary across-the-board reductions. That is why benchmarking should encompass the resources required to meet stakeholder and regulatory expectations, within the agreed-upon risk appetite for the organization.

Other reasons for benchmarking the internal audit function may be to examine use of outsourced vs. in-house resources, centralized vs. decentralized audit resources, career vs. rotational audit staffing, and frequency of audit coverage, as well as to identify differences in the level of audit services

provided compared to other organizations in the same industry.

### **STEP 2** Inventory Internal Audit's Principal Activities

Next, the CAE should inventory the principal activities performed by internal audit that may be handled differently within other organizations. For example, does internal audit run the U.S. Sarbanes-Oxley Act of 2002 project management office or perform independent testing to support required management Section 404 assertions? Does the internal audit function provide direct support to external auditing, including substantive testing not required for the organization's Sarbanes-Oxley assessment on internal control? Does the organization operate in a heavily regulated environment with prescriptive requirements for the internal audit function?

Internal audit is regarded as an organization's third line of defense, responsible for providing independent assurance. The three lines of defense model establishes responsibility for internal controls and how organizations can best establish and coordinate duties related to risk and control. It also states that the individual lines of defense should not be combined in a way that reduces effectiveness. Coordination helps minimize gaps and eliminate duplication of assigned duties. Understanding the makeup of responsibilities within the three lines of defense is an important first step in benchmarking the internal audit function.

When inventorying an internal audit department's activities, CAEs should include all discrete activities that require 10 percent or more of total available internal audit resources. Getting too granular makes effective benchmarking difficult.

# Adding value to the business is the top audit challenge of small and mid-size enterprises, according to MetricStream's State of Internal Audit 2018 – Impact and Opportunities.

## STEP 3 Know and Define the Industry

For some organizations this is relatively straightforward. For others it may be more difficult, particularly if the organization is engaged in disparate lines of business. For example, a technology manufacturing company may also own broadcast media. Auditors should choose the most representative industry or consider benchmarking against two or more separate industries if this seems more appropriate. Next, they should identify key competitors and industry trends that may impact the benchmarking exercise.

One of the best means of understanding industry culture is through industry-specific benchmarking groups. Formal and informal groups focused on internal audit and Sarbanes-Oxley benchmarking exist in several industries, including aviation, engineering and construction, financial services, manufacturing, news media, and retail. Participation in networking groups and reading industry-specific publications provides insight to the organization's industry and its culture. This is valuable to understand commonalities and differences to be considered in the benchmarking exercise. For example, are most competitors privately held when the organization is publicly traded? Does the organization operate internationally compared to competitors that operate primarily in the U.S. and Canada? Is the organization's industry expanding or contracting or deploying administrative functions off shore? What is the cultural expectation for internal audit? Does the industry see internal audit as a policing activity or the function that runs the Sarbanes-Oxley program? Is internal audit viewed as a source of talent and a business partner or a necessary evil and corporate overhead?

## STEP 4 Identify Benchmarking Alternatives

There are numerous approaches to benchmarking the internal audit department. Each of these has advantages and disadvantages, and some are easier than others to develop and execute.

**Simple Approach** The most common and easiest approach is to use a basic metric such as total revenue per auditor or number of employees per auditor. Generally, the numerator in the ratio is publicly available (for public companies) and requires only determining the number of auditors in an organization to complete the benchmark ratio. It's a quick and easy way to approximate audit coverage with others. Comparisons in this basic approach also are included in other benchmark approaches with richer data. Usefulness is relatively limited, however, as differences in audit coverage or business operations are not identified. At best, it can serve as a minimum guideline in establishing a base level of resources compared to other companies.

**Internal Audit Benchmarking Report** The IIA's benchmarking tool compares audit department size, experience, and other metrics against the averages of similar organizations in chosen peer groups. Benchmark metrics include employee compensation; organizational statistics; department staffing and costs; oversight, including audit committee information; operational measures, including audit life cycles; performance measures; and risk assessment and audit planning information.

Data is confidential and reported only in aggregate form. Identifying information is not publicly disclosed, although a list of participating companies within each industry is provided.

Once internal audit and the CAE make their benchmark metrics selections, the Audit Intelligence Suite compares the audit activity against comparable departments and creates a tailored benchmark report. Principal limitations are the fee and whether sufficient representation exists with companies of the same size and characteristics within the same industry.

**Private Benchmark Survey** Industry-focused and private benchmark surveys also provide relevance and credibility. An alternative is to use the peer group of organizations cited in most proxy statements for U.S. publicly listed companies. For example, the 2018 Fluor Corp. proxy listed 22 companies considered direct competitors and other peers in the engineering and construction industry. This is the perfect group to enlist for a private benchmark survey. To preserve anonymity and confidentiality, it may be useful to mask specific organization responses. An independent third party can facilitate collection and dissemination of results; specific categories can be banded to preserve confidentiality of individual responses.

Revenue can be grouped in broad categories and a similar approach can be used for internal audit budget amounts, number of employees, and other benchmark data. Audit committee members and executive management tend to view peer surveys as the most relevant as they compare companies with much of the same risks, industry constraints, culture, and regulatory requirements. The approach takes effort to execute and typically requires assistance from an independent third party to facilitate. Consequently, this benchmark exercise often takes longer than other approaches.

**Third-party Surveys** Most of the Big Four accounting firms, professional

service providers, and recruiters publish annual or periodic surveys covering internal auditing. It is worthwhile to research current publications and consider whether these can be used to benchmark the organization's internal audit function. However, it is sometimes difficult to apply broad surveys to satisfy the data requirements for a specific benchmarking exercise. In addition, third-party surveys often are thematic in focus, and do not provide sufficient demographic detail or include the necessary data to facilitate benchmarking internal audit resources and head count.

**It is sometimes difficult to apply broad surveys to satisfy the data requirements for a specific benchmarking exercise.**

**Appraisal Approach** The appraisal (or market adjusted) approach starts with basic survey data from another benchmark survey. Adjustments are then made to account for differences in the organization's inventory of audit services compared to others included in the basic survey. This concept is similar to the technique used by real estate appraisers where the individual property value is appraised based on the comparable value of nearby existing homes and adjusted upward or downward for such things as a pool, finished patio, and high street traffic.

When conducting an appraisal approach survey, CAEs should try to accumulate data on services that may not be comparable based on their knowledge of the industry, competitors, or the uniqueness of their organization. For example, if other organizations do not provide external audit direct assistance and

the organization provides three full-time exempt (FTE) employees, the CAE should subtract three FTEs from the head count comparisons in the benchmark survey, along with appropriate footnotes. This approach recognizes unique differences in audit services and attempts to provide a balanced, apples-to-apples comparison. It requires judgment and data to execute and can be subject to criticism by stakeholders if additions or subtractions appear arbitrary or not well-supported.

### **External Audit Fee Comparison**

There also is no standard to determine the appropriate amount to spend on external audit fees. These fees vary widely among organizations of equal size and are driven by the same organization control environment characteristics applicable to internal audit. This relationship holds true when external audit fees are market-driven (based on hours to complete the audit), which reflects complexities in the availability, quality, and reliability of data and the organization's control environment. Consequently, internal audit fees compared to external audit fees can be extrapolated across peer organizations to develop a range of expected internal audit spending for the organization.

This approach provides the most useful metric that reflects the unique characteristics and differences in organization control environments. External audit fees, along with organization revenue information, are available from U.S. publicly listed companies. Completion of this benchmark analysis requires obtaining the cost or head count for the internal audit function. Audit committees tend to like this comparison because it provides a snapshot of both internal and external audit fees, particularly if focused on organizations in the same industry.



# 40% of chief audit executives say internal audit has strong organizational impact and influence, according to Deloitte's 2018 survey, The Innovation Imperative.

## STEP 5 Summarize and Interpret Results

Once data has been collected, CAEs should summarize and apply results for the organization to the external benchmark survey. Stakeholders appreciate the insight of multiple perspectives that add credibility to the thoroughness of the exercise. Accordingly, CAEs should use as many approaches for obtaining benchmarking data as possible. This will provide a comprehensive snapshot of the organization's internal audit function and resources compared to others.

Stakeholders can compare spending in the organization's industry to other industries or organizations with similar revenue, and see differences in external audit fees and the categories of services provided by internal audit functions.

CAEs also can consolidate individual surveys to establish a range of acceptable internal audit resources and coverage that facilitates flexibility and judgment for making resource or staffing decisions. If the internal audit function is well above or below the range established by triangulating multiple surveys, compelling data now exists for recommending specific changes.

## STEP 6 Report Benchmark Results to Stakeholders


The CAE should approach reporting the results of a benchmark analysis with the same objectivity and rigor applied to internal audit reports. It's important to consider the assessment from the perspective of recipients, stakeholders, and decision-makers on the audit committee and in executive management. After the study is prepared, the preliminary results should be vetted with stakeholders to ensure key perspectives have not been

overlooked. Invariably, audit committees also will ask the external auditor for input, so he or she should be included in the vetting process.

The benchmark report from the CAE should describe the objectives of the exercise and the survey approaches used, along with any assumptions and exclusions. Transparency is imperative for the report to be viewed as objective and credible. CAEs should summarize relevant industry trends, cultural differences, variations in audit services provided by their function compared to others, and other data points stakeholders should be aware of. They should conclude with recommended changes based on benchmark data in line with stakeholder expectations for internal audit.

Frequently, the survey supports the current level of resources and head count without the need for substantive changes. Such a conclusion also provides value to the audit committee by independently corroborating the appropriateness of resources. Finally, CAEs should summarize survey results and disseminate them to other participants if industry or private benchmark surveys were conducted.

### OPPORTUNITY FOR DIALOGUE

All CAEs should right-size the internal audit function periodically to satisfy IIA Standard 2030: Resource Management. Benchmarking and comparison with other organizations also helps ensure the function provides reasonable value and coverage for the industry and company risk profile. It also affords an opportunity for insight and dialogue with the audit committee and management to sustain and grow investment in internal audit resources. 

---

**STEPHEN SHELTON, CPA, CISA, CCEP,** is senior vice president, internal audit, at Mr. Cooper Group (Nationstar Mortgage) in Coppell, Texas.



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

## Emerging technologies such as AI present a host of risks, and opportunities, for auditors to consider.

Michael Rose, Ethan Rojhani,  
and Vivek Rodrigues

Illustration by Sean Yates

**T**he “big” in big data hardly seems adequate to describe the scope of today’s digital information. Each day, the world produces 2.5 quintillion bytes of new data, according to a 2016 IBM Marketing Cloud report. In fact, 90 percent of data created over the history of the human race was generated in the past two years alone, the report says.

Increasingly, competitive advantage is driven by organizations’ ability to access, collect, synthesize, analyze, and exploit insights from that data. But the scope of this undertaking swamps traditional practices and capabilities. Tackling it effectively requires mastering emerging technologies, such as artificial intelligence (AI) and robotic process automation (RPA).

For internal auditors, these technologies present a challenge and an opportunity. The challenge? How can they help their businesses understand, codify, and develop appropriate controls around the new risks presented by RPA, AI, and other technologies? The opportunity? Where, within the internal audit function itself, can these tools be



the  
RISE



of Automation





leveraged to provide deeper insights with greater efficiency?

### EMERGING TECHNOLOGY RISK

AI and RPA have great potential to increase efficiency, but they also can help reduce organizational risk. Processes handled by these technologies are performed quickly and with absolute consistency; humans make mistakes or skip steps, robots do not. But that speed and consistency carries its own risk. If a faulty algorithm exists, if the tools access incorrect or incomplete data, if someone tampers with the process, or if RPA does not adjust to changing business or economic conditions, then the organization's automated processes can magnify human errors. Consequently, significant follow-up work may be required to unwind the errors.

Internal auditors should ask several questions when assessing risks associated with emerging technologies:

- » Has the organization established programs to take advantage of these technologies? Are foundational programs in place, such as data management and governance, as well as user-access controls?
- » Who is responsible for determining whether and how such tools can access the organization's data? Has clear accountability been established? Are appropriate safeguards in place?
- » Has the organization implemented appropriate development

and deployment controls, addressing issues such as how and when new processes are tested and updated?

- » Who is accountable for ensuring that use of the technologies complies with corporate policies, as well as applicable laws and regulations?
- » Are these processes being considered holistically to address change management, human resources, and other related concerns?

Additionally, internal auditors should determine what the organization is doing to ensure effective governance of its technology (see also "A New Age of IT Governance Risk" on page 20). Audit leaders need to work with organizational leadership to help develop an appropriate governance strategy for managing these technologies—and also to help unlock their potential. Internal auditing should be involved as part of the design or launch process so key risk indicators can be identified and appropriate controls embedded. This approach is far more effective than trying to append controls as an afterthought. Audit leadership can aid the chief technology officer and chief information officer in the development of a strong governance plan. Numerous available frameworks, such as COBIT and ITIL, can serve as guides. Also, guidance from the chief legal counsel and compliance department may provide additional support. The governance structure or plan over technology should be periodically reviewed for modifications that may be needed.

### THREE LINES OF DEFENSE

One of the challenges of today's rapidly changing business technology involves working effectively across the first and second lines of defense, while maintaining internal audit objectivity. The traditional audit



**Internal auditors should determine what the organization is doing to ensure effective governance of its technology.**



More than **90%** of managers and analysts **globally** expect new business value at their company from artificial intelligence in the coming five years, according to a recent *MIT Sloan Management Review* survey.

## AI AND RPA DEFINED

**D**efinitions of AI vary. *The English Oxford Living Dictionary* defines it broadly as: “The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.” RPA, on the other hand, involves the use of software with AI and machine learning capabilities to handle high-volume, repeatable tasks that previously required humans to perform. These tasks can include queries, calculations, and maintenance of records and transactions.

Consider the challenge of wading through potentially thousands of contracts that may contain embedded leases, in an effort to comply with the Financial Accounting Standards Board’s new lease accounting rules. Organizations currently use AI technologies such as text recognition and natural language processing to scan contracts for language that indicates an embedded lease may exist, and to flag those contracts for review. RPA is often coupled with this process to route flagged contracts to appropriate parties, ensuring decisions on embedded leases are made timely. Subsequently, RPA is also often used to follow up on, and to confirm, a decision has been made on those contracts. Beyond this narrow example, a variety of studies indicate that as much as 45 percent of the work performed in businesses every day could eventually be replaced by RPA.

approach incorporated relatively static, periodic risk assessments and statistical sampling of data from past transactions to identify control issues. Auditors often identified issues months or more after they arose, making remediation untimely and allowing losses or other issues to compound. With today’s tools, internal audit functions can test most or even all transactional data and can do so in close to real time.

The acceleration toward real-time auditing and the associated need to help identify and manage risks around emerging technologies means that internal auditors find themselves working more closely and more often with those in the first and second lines of defense. One of the benefits of real-time auditing involves pushing risk management down to the first line of defense wherever possible. Internal audit can play a key role in investigating how AI and RPA can be used to augment, and in many cases replace, current manual transaction testing and other risk-testing processes. Automating

control testing through the use of RPA can enable organizations to spot anomalies earlier.

An organization’s risk posture can be greatly improved by helping management understand the best uses of these tools and by working to deploy them in real time. The technology can help identify control deficiencies much sooner, enable testing of entire populations, and correct deficiencies immediately upon identification. As the third line of defense, however, internal audit needs to maintain its independence. Internal auditors may assist the first and second lines in establishing the use of these technologies by providing advice, but they must also ensure audit independence remains adequate to provide the additional layer of review.

### LEVERAGING THE TECHNOLOGY

When examining RPA and AI, internal audit shouldn’t limit its focus to the business’s use of these technologies. The audit function itself offers ample opportunities to leverage RPA and AI



# Trust Your Quality to the Experts

## Leverage an External Quality Assessment in 2019

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

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

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

# The robotic process automation market is forecast to increase by nearly 110% in 2019, according to Forrester Research's Predictions 2019: Automation.

to achieve efficiencies and improve results. Auditors should consider several potential applications:

- » Controls testing is a vital but time-consuming internal audit function, requiring consistent, repetitive application to be effective—just the sort of process that is ideally suited for RPA. In some cases, controls or testing processes will need to be modified to allow for RPA, but once it is in place, automation can produce accurate, consistent, and timely results. For example, ensuring the usefulness of data consumed from multiple sources historically would often require someone from the audit team to spend significant time stitching the data together. Today an RPA automation can quickly replicate all of those tasks with a higher level of accuracy.
- » Internal audit work requires a significant amount of routine, repetitive communication. For example, auditors often need to request information and then follow up on those requests, many of which are triggered by specific due dates. These processes offer key opportunities for automation.
- » Scorecard population, audit committee reporting, and other predictable documentation demands often can be fully or partially automated. Dashboards can be fully automated for management and the board of directors. Using RPA with a visualization tool can enable automated generation of dashboard information for these key stakeholder groups.

The specific opportunities to apply emerging technology to the internal

audit function will, of course, be partly determined by the circumstances of each organization. By seizing those opportunities where they exist, audit leaders can free up their professionals to focus on the critical thinking necessary to provide real strategic insights for the business.

Delivering those insights and managing the risks of emerging technologies also requires expanded skills—internal audit leaders should keep those needs in mind as they hire and train staff. Although technology can fuel significant improvements and efficiencies, deploying the right people, skills, and approach ultimately enables the technology to work as intended. Of course, a solid accounting and audit background remains

vital, but more and more skills around data science and IT must be part of the internal audit group. And the central mission of internal auditing—to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight—remains the same. But tools like AI and RPA require auditors to possess broader technological skills, strong data management capabilities, and familiarity with mathematics—such as linear algebra and statistics, which drive algorithm development. A background in coding also can be valuable.

Hiring professionals with these skills and training those already in the internal audit function is essential. Not only will it position the audit

team to best understand and address emerging technology risk, but audit functions considered leaders in these areas may be seen as more attractive to top talent.

## PARTNERS IN TRANSFORMATION

The emergence of AI, RPA, and similar technologies is much like that of spreadsheet applications in the mid-1980s. Spreadsheets at that time were innovative and useful, but not yet widely adopted. Within 10 years, they became ubiquitous and revolutionized work, not only within internal audit but across the business world.

Likewise, AI and RPA are transforming businesses and their internal audit functions. And while the new technologies present new risks, these

## Effectively managing emerging technology risks while also leveraging AI and RPA tools are key challenges.

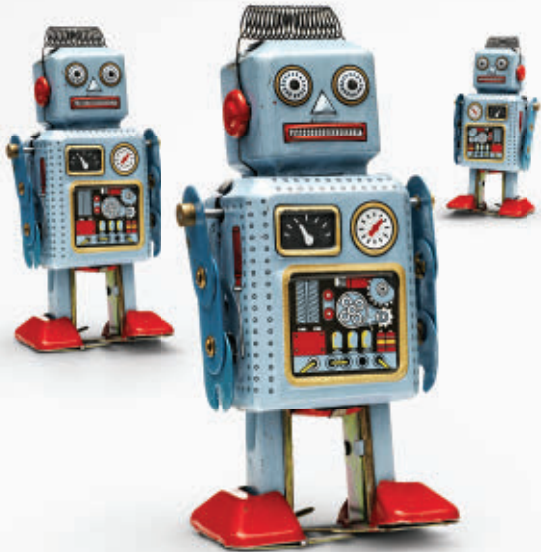
risks can be managed. The greater risk is failing to capitalize on the power and utility AI and RPA tools offer. Effectively managing emerging technology risks while also leveraging these tools are key challenges for today's internal audit leaders. By doing so, however, they can become true strategic partners in their organization's success. [▶](#)

**MICHAEL ROSE, CIA, CPA, CISA, CISM**, is a Business Risk Services partner at Grant Thornton LLP in New York.

**ETHAN ROJHANI, CISSP, CPA, CFE, CGFM**, is a Business Risk Services partner at Grant Thornton in Denver.

**VIVEK RODRIGUES** is a Digital Transformation and Management senior manager at Grant Thornton in New York.

STATUS QUO IS ONE OF MANY.



**Status Go**<sup>™</sup>  
IS ONE-ON-ONE.

Ready for an approach that's as  
unique as it is personal?

**Welcome to Status Go.**

[gt.com/statusgo](https://gt.com/statusgo)

 **Grant Thornton** | Audit | Tax | Advisory

"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the independent network of GTIL member firms provide services to their clients, as the context requires. GTIL and each of its member firms are not a worldwide partnership and are not liable for one another's acts or omissions. In the United States, visit [grantthornton.com](https://grantthornton.com) for details. © 2017 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd



# *Penalizing Corruption*

The U.S. Securities and Exchange Commission's Whistleblower Program has fined companies more than \$1 billion since 2011.

# S

ince its inception, the U.S. Securities and Exchange Commission (SEC) Whistleblower Program has fined wrongdoers more than \$1.7 billion. "Whistleblowers have played a crucial role in the progression of many investigations and the success of enforcement actions," said Jane Norberg, SEC chief of the Whistleblower Program, following the \$16 million payout to two whistleblowers in November 2017.

The SEC's 2017 Annual Report to Congress on the Whistleblower Program provides insights for internal auditors and audit committees into the program's scope, focus, and results. In 2017, the SEC awarded approximately \$50 million to 12 individuals for various whistleblower actions. These reports included providing information about a fraud arrangement that was difficult to detect, disrupting investment schemes that targeted unsophisticated investors, and supplying industry-specific information. Norberg stressed the three key features of the program are monetary rewards for information that leads to successful enforced actions, anti-retaliation protections, and confidentiality safeguards.

Given the growing impact of the SEC Whistleblower Program, internal auditors should encourage executives and directors who oversee governance to understand the key elements of the program. Moreover, auditors should ensure

**Daniel Gaydon**  
**Douglas M. Boyle**



internal processes and controls are in place to effectively resolve whistleblower concerns and build employee trust.

### WHISTLEBLOWER INCENTIVES

The SEC Whistleblower Program was created in 2011, as directed by Section 922 of the U.S. Dodd-Frank Wall Street Reform and Consumer Protection Act, to provide incentives to whistleblowers to report federal securities law violations. Section 21F allows rewards for individuals who provide information that leads to a successful SEC enforcement action resulting

49 percent since 2012, reaching an all-time high in 2017. The categories that have remained the highest over the life of the program include corporate disclosure, offering fraud, and manipulation (see “Whistleblower Allegation Types” on page 46).

Approximately 68 percent of TCRs submitted in 2017 came from the U.S., 20 percent from international locations, and 12 percent from a location not disclosed. The annual number of TCRs submitted internationally has grown 75 percent since 2012.

Although the Dodd-Frank Act prohibits the SEC from disclosing the identity of the whistleblower, the commission does publish the roles in which the whistleblowers served in aggregate. In 2017, most award recipients were current (30 percent) or former employees (25 percent). The remaining recipients included harmed investors (19 percent), outsiders (15 percent), other insiders (7 percent), and industry professionals (4 percent).

Not only are the TCRs up, the amount paid to whistleblowers from the Investor Protection Fund also has been increasing. The SEC has awarded more than \$60 million to whistleblowers since 2012 (see “The Top Whistleblower Awards” on page 47).

### PROTECTING WHISTLEBLOWERS

With the monetary awards and payouts growing each year, the SEC has emphasized whistleblower protection since 2017. In separate instances, the SEC levied \$2.4 million in penalties against publicly listed companies that retaliated against or hindered employees’ ability to report potential violations to the commission.

Specifically, Section 21F(h)(1) of the Dodd-Frank Act provides whistleblowers with protection against retaliation. In addition, Exchange Act Rule 21F-17(a) forbids employers from not allowing employees to report securities

## The SEC has received more than 22,000 tips, complaints, and referrals.

in sanctions greater than \$1 million. Whistleblowers may be an employee, an insider such as a consultant, or an outsider of the company.

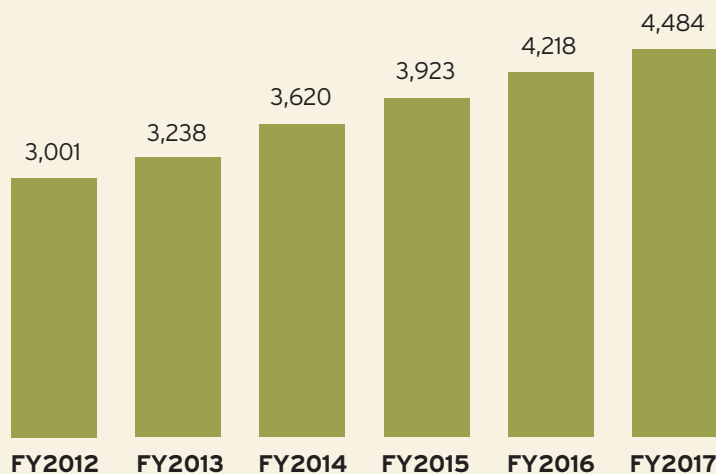
Whistleblowers are eligible for payments of 10 percent to 30 percent of the monetary sanctions collected. To receive payment, the whistleblower must complete the award application within 90 days of when the SEC Notice of Covered Action is posted. Factors that could increase the payment amount include how vital the information is to the SEC action, higher level of cooperation, and evidence the violation was first reported through the company’s internal network. Inversely, factors that could decrease payment include the whistleblower’s involvement in the violation and significant delay in reporting the violation.

### PROGRAM GROWTH

Since the whistleblower rules took effect in 2011, the SEC has received more than 22,000 tips, complaints, and referrals (TCRs). “Whistleblower Tips” on page 45 shows that TCRs have risen

The SEC Whistleblower Program has **recovered** \$671 million in **ill-gotten gains** and interest since 2011, most of which has, or will be, returned to harmed investors, the SEC says.

## WHISTLEBLOWER TIPS



Source: SEC's 2017 Annual Report to Congress on the Whistleblower Program

violations to the SEC. The act states that “no person may take any action to impede an individual from communicating directly with the commission staff about a possible securities violation, including enforcing, or threatening to enforce, a confidentiality agreement ... with respect to such communications.” The SEC can take legal action against employers that retaliate against employees for reporting federal securities law violations.

In 2017, the SEC found numerous violations of Rule 21F-17(a). For example, Washington, D.C.-based financial service firm Homestreet Inc. agreed to pay a \$500,000 penalty for attempting to identify a whistleblower following an SEC inquiry into accounting violations. Moreover, the SEC found that Homestreet employees were only eligible for severance benefits if they signed an agreement waiving potential whistleblower rewards.

The SEC also brought actions against companies for implementing restrictive covenants in their severance and termination agreements. In January

2017, BlackRock Inc. agreed to pay a \$340,000 penalty for including inappropriate language in its separation contracts. In exchange for monetary payments, more than 1,000 former employees signed agreements waiving “any right to recovery of incentives for reporting misconduct, including, without limitation, under the Dodd-Frank Wall Street Reform and Consumer Protection Act.”

In another example, the SEC found Oklahoma energy company SandRidge Energy Inc. had violated

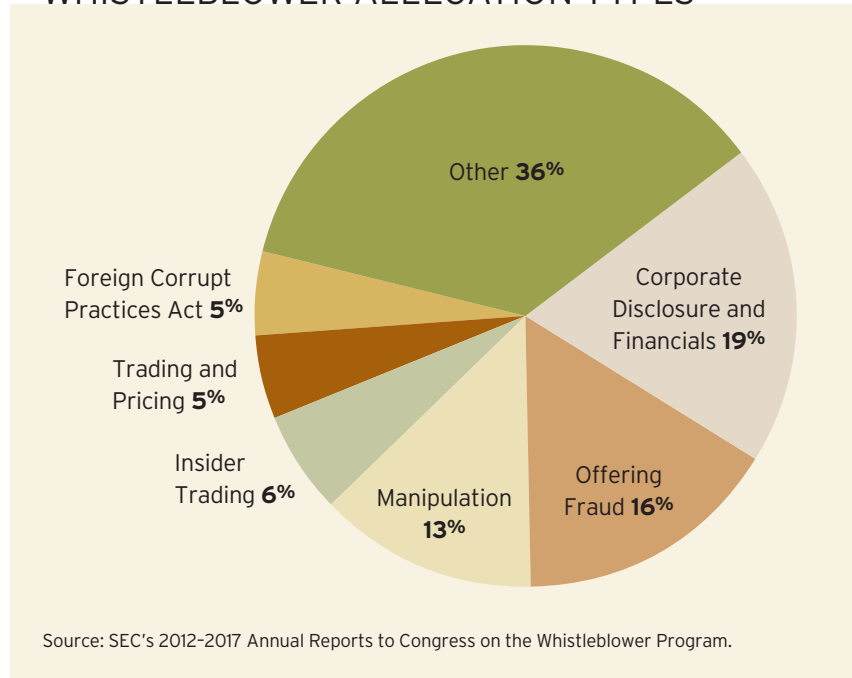


For more information about the SEC Office of the Whistleblower Program, VISIT [www.sec.gov/whistleblower](http://www.sec.gov/whistleblower)

## The SEC can act against employers that retaliate against employees.

both Rule 21F-17(a) and the whistleblower anti-retaliation provisions of Section 21F(h). SandRidge terminated an employee after the whistleblower expressed concerns regarding a reserve calculation. In addition, more than 500 former SandRidge employees signed separation agreements from August

### WHISTLEBLOWER ALLEGATION TYPES



2011 to April 2015 that prevented them from disclosing information to any governmental agency regarding company investigations. SandRidge agreed to pay \$1.4 million in penalties.

Internal auditors may help the organization define, monitor, and manage elements of the whistleblower process to ensure an effective and appropriate

Moreover, these penalties could result in a scandal that causes reputational damage to the companies involved. In an August 2014 press release, former SEC Whistleblower Office Chief Sean McKessy stressed the importance of internal auditors. "Individuals who perform internal audit, compliance, and legal functions for companies are on the front lines in the battle against fraud and corruption," he said. "They often are privy to the very kinds of specific, timely, and credible information that can prevent an imminent fraud or stop an ongoing one."

In some cases, internal auditors, themselves, may be whistleblowers. In 2014 and 2015, the SEC awarded whistleblower rewards to employees within compliance and internal audit functions. According to Section 21F-4, if internal auditors come across a violation, they should first report it internally to the appropriate officer or board member. If action is not taken within

**Auditors can review whether claims were resolved appropriately.**

avenue is provided to report claims. Auditors also can review whether claims were resolved appropriately.

**INTERNAL AUDIT IMPLICATIONS**

With more than \$1 billion in penalties levied so far against companies, the SEC Whistleblower Program is having a significant impact in monetary terms.



The SEC took **2+ years** on average to make **decisions** on whistleblower claims from 2014 to 2017, compared to one year in 2012 and 2013, according to a *Wall Street Journal* analysis of SEC releases.

## THE TOP WHISTLEBLOWER AWARDS

Below are the largest whistleblower rewards issued by the SEC since the whistleblower program's inception. Nine of the top rewards occurred during 2016 to 2018.

RELEASE DATE	AWARD AMOUNT	SEC QUOTE
March 19, 2018	<b>\$49 million</b>	<i>The whistleblowers "provided critical information that advanced the first investigation, including the identification of potentially relevant documents and key witnesses."</i>
Sept. 6, 2018	<b>\$39 million</b>	<i>The whistleblower "voluntarily provided original information to the commission that led to the successful enforcement of the covered action."</i>
March 19, 2018	<b>\$33 million</b>	<i>"The information was previously unknown to the staff handling the investigation that resulted in the covered action."</i>
Sept. 22, 2014	<b>\$30 million</b>	<i>"The whistleblower came to us with information about an ongoing fraud that would have been very difficult to detect."</i>
Aug. 30, 2016	<b>\$22 million</b>	<i>"Whistleblower whose detailed tip and extensive assistance helped the agency halt a well-hidden fraud at the company where the whistleblower worked."</i>
Nov. 14, 2016	<b>\$20 million</b>	<i>"This whistleblower alerted us with a valuable tip that led to a near total recovery of investor funds."</i>
June 9, 2016	<b>\$17 million</b>	<i>"The information and assistance provided by this whistleblower enabled our enforcement staff to conserve time and resources and gather strong evidence supporting our case."</i>
Sept. 6, 2018	<b>\$15 million</b>	<i>The whistleblower "appeared before the agency for an investigative interview."</i>
Oct. 1, 2013	<b>\$14 million</b>	<i>"The whistleblower(s)' information led to SEC enforcement action that recovered substantial investor funds."</i>
Nov. 30, 2017	<b>\$8 million</b>	<i>"The whistleblower alerted SEC enforcement staff of the particular misconduct that would become the focus of the staff's investigation and the cornerstone of the agency's subsequent enforcement action."</i>
Nov. 30, 2017	<b>\$8 million</b>	<i>"The whistleblower provided additional significant information and ongoing cooperation to the staff during the investigation that saved a substantial amount of time and agency resources."</i>

Sources: SEC orders and press releases related to the whistleblower program

# A New Look at Internal Auditing.



## Audit Intelligence Suite

Benchmark | Assess | Survey

**Benchmark your audit function**, assess your team, and survey your key stakeholders. Once you know the results, you will be in a better position to improve your audit function.

**Learn More**

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



AUDIT EXECUTIVE  
— CENTER® —

In June, the SEC proposed a **rule** that would **reduce** whistleblower **awards** that are based on penalties of \$100 million or more to “more appropriately and expeditiously” reward whistleblowers.

120 days, the internal auditor becomes eligible for an award and may begin the whistleblower process by reporting either through the SEC’s online questionnaire or by completing a hard copy Form-TCR.

Because more than half of whistleblower reports come from company insiders, chief audit executives (CAEs) should work closely with the audit committee to ensure the appropriate tone, policies, and diligence are in place to support a whistleblower who first reports internally. In “Whistleblowers: What the Board Needs to Know,” The IIA’s Tone at the Top newsletter lists six steps that boards and CAEs should take to oversee a whistleblower program:

- » Build employee trust of internal policies.

- » Consider all sources, including hotlines, anonymous email, lawsuits, exit interviews, and social media.
- » Ensure adequate triage of the report based on understanding the legal and accounting implications.
- » Enlist internal audit in managing the whistleblower process, managing the investigative process, or reviewing whistleblower activities.
- » Understand the entire whistleblower program process.
- » Remain vigilant by continually reviewing and updating whistleblower policies.

The SEC Whistleblower Program has resulted in increased tips, fines, awards, and whistleblower protections.

With the monetary rewards increasing, reports to the SEC’s Whistleblower Program are likely to grow. Against this backdrop, internal auditors can help their organization’s whistleblower program through education, communication, and monitoring. Given their knowledge of the organization’s governance, policies, and procedures, internal audit’s involvement can add credibility to the whistleblower program. However, auditors should remain objective and leave decision-making responsibility about specific whistleblower cases to management. [la](#)

**DANIEL GAYDON** is a doctorate student at the University of Scranton in Pennsylvania.

**DOUGLAS M. BOYLE, DBA, CPA, CMA,** is accounting department chair and associate professor at the University of Scranton.

## YOU *Are* INVITED

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

UPCOMING 2019 VISION UNIVERSITY SESSIONS:

**Orlando, FL**  
Feb. 26–March 1

**Boston, MA**  
June 24–27

**San Diego, CA**  
Sept. 9–12

**Chicago, IL**  
Nov. 19–22

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

CAE Success in a Class All Its Own

**VISION UNIVERSITY**



**AUDIT EXECUTIVE  
CENTER®**

2018-1402

Relevant. Reliable. Responsive.



## SHARPEN YOUR FOCUS

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

Print | Online | Mobile | Social

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

**Ia**  
INTERNAL AUDITOR



# Breaking free of mental traps

Internal auditors can take steps to avoid overthinking that can affect audits and service to clients.

Murray D. Wolfe

**F**eeling caught in a mental trap? Overthinking can inhibit internal auditors' service to clients. "Mental traps are habitual modes of thinking that disturb our ease, take up enormous amounts of our time, and deplete our energy, without accomplishing anything of value," former University of Toronto philosophy and psychology professor André Kukla writes in *Mental Traps: The Overthinker's Guide to a Happier Life*.

Auditors can unwittingly fall into many mental traps and "spin" at any point in the engagement



life cycle. Being aware of these traps and learning how to overcome them can help auditors become better at their jobs, reduce the effort required to finish their work, and deliver greater value to their clients.

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

Among the mental traps that the book covers, nine are most relevant for internal auditors: persistence, amplification, fixation, reversion, anticipation, procrastination, acceleration, resistance, and division. According to Kukla, each of these traps relates to four cardinal errors pertaining to undertaking tasks or projects: Individuals either do too much or too little, or they start or finish a task too soon or too late. Internal auditors should be mindful of these traps and errors and take proactive steps to manage them.

**PERSISTENCE** The first trap involves continuing to work on tasks that have lost their value. This results in people doing too much.

As Kukla points out, North American culture teaches people to

It is important to remember, however, that there is a difference between persistence and perseverance. While persistence is a mental trap that leads to a dead end, perseverance is a laudable trait in which one steadfastly pursues a goal despite encountering obstacles.

**AMPLIFICATION** Working harder than necessary to achieve one's aims and doing too much is amplification. For internal auditors, amplification occurs in a few common situations. The first is when they continue testing to prove an observation for which they have already collected sufficient evidence. After all, if some evidence is good, more must be better, right?

Auditors can avoid this by applying a rule of thumb: Only gather enough evidence to convince the intended audience to take action. Once the threshold is reached, quit digging.

Engaging in "analysis paralysis" is another example. This occurs when internal auditors continue to analyze a situation beyond what is required in the belief that it will help make the case for change.

Internal auditors also can spend inordinate time polishing reports because they believe the reports are not ready. Auditors face the law of diminishing returns and at some point need to stop the work and issue the report. They don't need to be perfect. Setting relatively firm deadlines can help auditors deal with this mental trap.

**FIXATION** Related to amplification, fixation occurs when progress toward finishing an engagement or task is blocked. This often occurs when internal auditors require additional information from a stakeholder such as an executive who happens to be unavailable.

Instead of using the time to do something else that will help complete the engagement, auditors may waste

**While persistence is a mental trap that leads to a dead end, perseverance is a laudable trait in which one pursues a goal despite encountering obstacles.**

regard persistence as a virtue. This is a form of mental inertia—having begun an activity, people keep moving in the same psychological direction until they reach the end. This inertia tips the scale in favor of continuing the task even if it no longer has merit. The individual promised to complete it, so he or she will doggedly carry on to the end.

“Mental traps are identified not by the content of our ideas but by their form,” according to *Mental Traps: The Overthinker’s Guide to a Happy Life*, by André Kukla.

time by devoting efforts to activities that add no value or repeating what’s already been done. Neither of these actions ultimately adds any value. As a result, auditors expend too much effort on the current task and don’t begin the next task soon enough. Auditors can avoid this situation by effectively planning for the future and considering the schedules of key stakeholders.

**REVERSION** A bit more complex, reversion happens when people have set out to accomplish a task and have failed at it. Rather than let it go, they continue to focus their thoughts on attaining the missed goal. Kukla states that “reversion is the temporal opposite of fixation,” but rather than working to hasten an *immovable future* when a task is blocked, people try to change the *immutable past*.

Fixation and reversion share a common problem in that people continue to work on a task when there is nothing more to be done. With reversion, auditors need to accept their failure; get over the feelings of guilt, regret, or shame; and move on to the next project.

**ANTICIPATION** Auditors can suffer from anticipation by starting a task too soon—for example, by not planning enough before they begin fieldwork.

Inexperienced internal auditors are prone to the anticipation trap by being anxious to start fieldwork before they understand why the engagement is being undertaken, what is the most effective way of obtaining evidence, and how the engagement should be executed to meet the clients’ needs. This is evident when auditors begin detailed testing of transactions before exploring other, less labor-intensive options, such as interviews or walk-throughs, to get evidence. Internal auditors need to plan adequately before beginning fieldwork, yet not do

so much planning that they delay getting started.

**PROCRASTINATION** One of the most prevalent mental traps, procrastination involves performing small, relatively meaningless tasks that take the place of actually devoting time to required or appointed tasks that will add value. Engaging in procrastination, internal auditors end a current task too late and do not start the next task soon enough.

One common way of procrastinating is to postpone starting fieldwork by over-planning. Auditors can avoid this

the engagement report the moment fieldwork begins. Doing so promotes refining and testing observations and conclusions as the engagement progresses rather than waiting until the end.

Although related to amplification, performing more tests than required during fieldwork can be another form of procrastinating. This can be the case when additional testing is done to avoid getting to the next phase of the engagement.

**ACCELERATION** The flip side of procrastination is acceleration. Rather than being slow to start, acceleration

Anticipation involves starting a task too soon. Internal auditors can suffer from this trap by not planning enough before they begin fieldwork.

by establishing deadlines and allocated efforts for each phase of the audit and holding to them as much as possible. Some flexibility is needed, of course, but an audit is a small project and should be treated like one.

Another way to procrastinate is to delay contacting stakeholders to avoid confrontation or a potentially unpleasant discussion. Auditors may delay for a day or two, only to find out that the stakeholder is not available for the next week. If this happens enough times, the engagement timeline can be delayed by several weeks.

Internal auditors also procrastinate by not writing their audit report because they know writing, editing, and finalizing it will open themselves to challenge and criticism from their supervisors and clients. Audit departments can address this trap by beginning to draft

occurs when people don’t give a task the necessary time and attention and end up finishing it too soon. Often, procrastinating at the beginning of a project or task can result in acceleration at the end.

For example, internal auditors may rush through planning, ultimately not delivering what clients and stakeholders wanted. As a result, they may have to go back and perform more unplanned fieldwork. Failing to take time to ensure tests are designed appropriately and executed correctly may yield faulty evidence from rushed and sloppy work. Auditors also may have to repeatedly revise reports because they rushed to write a first draft without adequately thinking through what they want to report on and how they want to report it.

Internal auditors can avoid acceleration by devoting time to

# IIA Training Stations

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



## Learn From The Leader.

.....  
**IIA TRAINING – ALL PLATFORMS OPEN**

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

Schedule training on a platform perfect for your station [www.theiia.org/Training](http://www.theiia.org/Training)





perform each phase of audit work effectively through appropriate planning and continually monitoring their progress throughout the engagement. Frequently referring to the scoping document throughout the audit — especially when writing the report — can help keep internal auditors on track and focused on the goal of the engagement.

**RESISTANCE** When people who are busily involved in a task that is going well are presented with a valid emergency, opportunity, or interruption that requires their attention, resistance occurs. This could include a client request for an urgent, high priority, and inconvenient assignment while auditors are in the middle of another engagement. An example could be an unplanned investigation into a fraud at a remote location that will require significant travel and time away from home. To address this trap, auditors can apply a general rule proposed by Kukla: “It is pointless to let opportunity slip away when the present task can be postponed without cost.”

**DIVISION** The division trap happens when individuals try to concentrate on two things at once. This trap involves the mistaken assumption that people can be effective multitaskers.

Kukla points out that people cannot consciously attend to two things at once because attention is indivisible. When individuals think they are multitasking, they are either “fast-switching” their consciousness between two activities, or they have relegated one of the activities to an unconscious, automatic mode of operation.

Internal auditors, especially those at a senior level, often need to juggle many tasks. They rarely have the luxury of focusing on only one thing at a time. The problem is that dividing attention


between tasks actually takes more time and effort than concentrating on one task at a time. When people drop one task and return to it later, they don’t pick up at the spot where they left off. They have to spend time picking up the threads of the task.

To manage their time better, internal auditors should devote segments of time to specific tasks. They should take steps to avoid unnecessary

**By being mindful of mental traps and taking steps to break free of them, internal auditors can better enjoy their work and be more effective.**

distractions such as emails, telephone calls, and interruptions by direct reports or other employees. As Kukla notes, there is always something that can take a person’s attention away from the task at hand.

#### **A VIRTUOUS HABIT**

By being mindful of mental traps and taking steps to break free of them, internal auditors can better enjoy their work and be more effective in their roles. The aim is to devote less time and effort to producing consistently good results. Being mindful of mental traps is an ongoing discipline that can become a virtuous habit incorporated into auditors’ day-to-day work. It can supplement the well-developed technical skills and knowledge auditors already possess, helping to make them more successful as individuals and as team members. 

**MURRAY D. WOLFE, CRMA, CPA, CA**, is director, Internal Audit, at a large agricultural cooperative in Calgary, Alberta.

A university and health-care company partnered to create an internal audit internship program that equips students to hit the ground running.

# Real-world

**B**usiness schools across the country emphasize the importance of hands-on learning experiences via internship programs. Internal audit internships can provide students with an understanding of the business as a whole, allowing interns to get a clearer idea of areas that interest them. Additionally, internships in internal auditing expose students to various functional areas within a company so they can experience different career paths outside of their degree or major.

With an ambitious timeline for developing internal audit programs for multiple departments, Professional Physical Therapy (PPT)—an outpatient therapy provider in the U.S.—first collaborated with Hofstra University in Hempstead, N.Y., to offer a summer internship program in 2017. The goal of the internship program was not only to attract high-quality graduates to PPT, but

to attract candidates to the internal audit profession. More specifically, the objective of the internship program was to give students an opportunity to gain experience in the internal audit department of a large health-care company and refine their critical thinking skills as they relate to compliance and internal auditing. Unlike other internships that give detailed instructions on each task to be performed, this program was intended to give interns considerable autonomy.

As part of the program, PPT wanted the interns to develop department-specific audit tools for human resources, marketing, business relations/sales, and finance and accounting that were statistically viable and measured the overall performance, functional task compliance, and inherent risk associated with each department. Other objectives were to determine functional variability and level of error or noncompliance with legal, regulatory, operational, industry, and firm standards.





# Education

## SELECTION AND ONBOARDING

Hofstra faculty chose eight high-quality undergraduate and graduate student internship prospects. After interviewing with PPT's director of internal audit and chief compliance officer (CCO), all eight students were offered paid internship positions. The interns comprised four graduate students and four undergraduate students with majors in accounting, legal studies in business, biology, and marketing.

In the first week, interns participated in an orientation training boot camp. They were introduced to PPT staff and provided with an overview of the program, health-care internal audit best practices, and the organizational charts of the four departments to be audited. To help the interns understand what an audit looks like, they were provided with an overview of the PPT clinic and revenue cycle operation audits (i.e., how they were developed, scoring, performance, reports, and corrective actions). Interns were then assigned to one of the four

departmental internal audit teams and provided work stations.

Next, interns were assigned to project managers/mentors from the legal and compliance department in teams of two. Because the internship program took place in the health-care sector, interns were also provided with an overview of the U.S. Health Insurance Portability Accountability Act. Then they were trained on how to develop internal audit tools and given goals and deadlines for deliverables.

Guidance was given on how interns could access relevant information to achieve their objectives. For example, they were given job descriptions of individuals in the departments to be audited, relevant forms and policies, and the necessary steps to develop an audit tool. Also, interns were told they would be interviewing staff in the various departments to learn about departmental processes and role-specific job requirements. The legal and compliance team explained legal issues relevant to health care and the audit process

**Rina M. Hirsch**

ANDREYARKUSHA / SHUTTERSTOCK.COM

using an actual clinic audit, sample audit report, and corrective actions.

Finally, each audit team developed a 60-day plan that was reviewed by a mentor, conducted mock staff interviews to illustrate how interns should interview PPT staff, and learned how to research industry standards and best practices. Interns met with their mentors, who gave an overview of the timeline for internship components, including research, interviews, policy review, document review, internal audit tool development, testing, measurement and weighting, and audit performance.

**AUDIT TOOL DEVELOPMENT**

Teams were assigned to specific departments based on interns’ educational backgrounds and interests. The goal of having two-person teams was multifaceted. The interns were able to work as autonomous teams, while mentors provided guidance as needed. However, the interns relied on each other’s strengths to a great extent to achieve objectives before resorting to their mentor for guidance. This helped build interns’ self-confidence and reduced heavy reliance on mentors in the program.

audit tools, which consisted of binary questions that could easily be scored and weighted. Audit tool question development went through multiple steps of evaluation over a four-week period. First, the audit tools were approved by the project manager/mentor. Next, they were approved by the director of internal audit and then the CCO. Once a team received final approval, the interns conducted an audit using their newly developed audit tool. Based on those findings, the teams created key performance indicators (KPIs) and a KPI dashboard for each department audited.

With results from the audit and KPI information in hand, the interns prepared an audit report summarizing their findings. Interns also conducted a gap analysis and provided an action plan based on its results. Finally, each team prepared a presentation of its audit findings and presented them to PPT’s executive board.

**COMPANY BENEFITS**

The program allowed for an ambitious project of developing audit tools for continued use for four departments, and it was completed in a relatively short time frame. Furthermore, the review process in place (i.e., by mentors, the director of internal audit, and the CCO) ensured that the output of the program was of high quality. Because interns were responsible for the development of each department audit tool from start to finish, the project cost much less than it would have cost had it been performed by legal and compliance personnel.

The PPT internship program was such a positive experience for the members of the legal and compliance departments that PPT decided to hire one of the interns in a full-time capacity. Due to the success of this internship program, PPT’s director of internal audit and CCO indicated

The review process in place ensured that the output of the program was of high quality.

The interns’ first task was to gather research by reviewing industry and firm standards, firm policies and procedures, and relevant laws and regulations, and by interviewing respective department personnel. Each team’s mentor reviewed the information and aided or provided feedback to the interns as needed through the research process.

Once the research process was complete, the teams developed the



The average **conversion rate** of intern to full-time hire is **45.6%**, according to the National Association of Colleges and Employers' 2018 Internship & Co-op Survey Report.

interest in pursuing additional internships in the future.

The internship program increased exposure to, and promotion of, the company through the interns. By providing a positive and satisfying learning experience for the interns, the company receives positive publicity spread by the interns to their peers.

### STUDENT BENEFITS

Because each team was responsible for a project from start to finish, they were able to improve their critical thinking skills considerably by way of firsthand learning. By providing each intern with autonomy—and another intern to work closely with—they were able to bounce ideas off of one another to solve problems and achieve their objectives. Interns used critical thinking skills at every stage of the internship program: research, development, execution, reporting, and presentation. In addition to improved critical thinking skills, interns also refined their technical skills by using Excel tools and learned a great deal about health-care industry standards, departmental company standards, and best practices.

However, one of the greatest outcomes of the program was the opportunity for the interns to develop their communication and soft skills by placing them in real-world situations. Interns learned how to develop good rapport with company personnel, work efficiently as a team, capitalize on each other's strengths, and work under pressure. Feedback provided to the interns from mentors resulted in significant improvement in these areas. As a result, this internship program created much more desirable job candidates.

Interns in the program completed a mid-internship self-performance appraisal form where many indicated they were able to apply knowledge from their university studies to a real-world setting, learned a great deal


about areas in which they had very little previous knowledge, identified technical and presentation skills as being enhanced, and expressed that their communication skills improved. While several interns were frustrated with the real-world phenomenon of

**Internal audit internships can create positive experiences and enhance the perception of the profession.**

different expectations from different supervisors, they learned to cope with these sometimes-contradictory expectations. This reflects a clear acknowledgement of improvement in soft skills in the workplace.

The interns also identified gaining work experience in the health-care industry, working independently and within a team, and being responsible and accountable for work performed as additional benefits of the program. After presenting their findings to the executive board, interns indicated they felt a great sense of accomplishment and self-satisfaction.

### CHANGING PERCEPTIONS

Internship opportunities in internal auditing that create positive experiences for the interns and the organization can work to enhance perceptions of the internal audit profession. Students share their experiences with peers, which can translate to increased interest from students looking to learn more about internal auditing. Additionally, organizations may see an increase in high-quality candidates who may have never considered a career in internal auditing. 

**RINA M. HIRSCH, PHD, CPA**, is an assistant professor of accounting at Hofstra University in Hempstead, N.Y.



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

# Governance Perspectives

BY JUSTIN STROUD    EDITED BY KAYLA FLANDERS

## STARTING SMALL

Launching a one-person audit function takes patience, focus, and relationship building.

Several years ago, my employer, Western Reserve Group, a property and casualty insurer based in Wooster, Ohio, was contemplating the best way to launch an internal audit department—either in-house or outsourced. With continued growth of the company expected, it made sense to enhance its focus on internal auditing.

The company chose to outsource internal audit to third-party consultants. The consultants completed, on average, three to four audits per year, until about four years ago when senior management and the audit committee determined that having an internal auditor on site to manage the internal audit function, using a cosourcing model for technical expertise, was the best fit for the company.

I was brought on as that internal audit manager. As a one-person department, getting a positive start was a must. Recommending

wholesale changes to an already successful company would not be the best way to gain support for internal audit. Instead, I garnered support by listening to and observing the business units, while gaining some early wins by updating governance items, such as the internal audit charter and manual.

Absorbing knowledge from the business units helped expand my awareness of the organization and provided valuable insight down the road. Reviewing each of the audit reports completed by the prior consultants also was valuable. Likewise, reading the external auditors' and regulators' reports provided useful information in gaining a foundational knowledge of the organization.

Most important to developing an effective internal audit function is having a strong tone at the top that governance and internal audit go hand-in-hand in establishing the values and ethical behavior that guide

the organization. The support of the audit committee and CEO is vital in showing internal audit can be used as a valuable tool and resource, in addition to providing the typical assurances required. Since the first day, the continued support I have received has allowed internal audit to develop and grow. As Western Reserve's president and CEO Kevin Day puts it, "Strong corporate governance starts at the top of our organization with a focus on providing an ethical climate based upon our strong core values. It was vital when bringing an internal auditor on board that the entire company was aware the internal audit function was fully supported by the CEO and the board. We succeeded in this through transparency and communication throughout not only the management team, but also through all levels of the organization."

A saying I like to use is: "Look back to move forward." I saw where internal

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



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

audit was and then determined ways to improve the cycle time between audits of the core business areas and ensure high-risk areas were covered. Creating a function that adheres to the *International Standards for the Professional Practice of Internal Auditing* was a focal point.

Just determining each auditable function and the controls surrounding those areas can take considerable time and resources. The key is to be patient while continually moving forward in building an audit universe. From there, a risk-based audit plan can be formed while gathering trends and hot topics by interviewing key members of senior management to gain an overall picture of the organization. Blending that with industry-specific needs and audit focal points can help form a solid audit plan.

Internal audit must work as a strategic partner with management and should interact with all levels of the organization to gain support and show that it can be a trusted advisor. This cannot be accomplished in days or weeks, but rather in months and years, as trust will be built over time.

At times, it can feel like internal audit is spinning its wheels or going in many different directions at the same time.

It is human nature to overestimate what can be completed in one year or less, but people often greatly *underestimate* what they can complete in five years. Internal audit should start with a long-term road map that it frequently adjusts and reviews.

With limited resources comes limited time, but small audit functions must maintain flexibility when events occur that are outside the scope of the audit plan. Having laser focus and a detailed game plan can help squeeze in work that can add value to the organization.

Whether it is gaining certifications, frequently attending training events, or reading articles about the industry or profession, continuous learning also is important with the ever-changing risk environments of most organizations today and cannot be minimized in a small audit department.

It should be a goal of all internal audit functions, regardless of size, to ensure adequate coverage across the organization's audit universe. But internal audit must first understand where all the risks and their respective control points occur. [la](#)

**JUSTIN STROUD, CIA, CRMA, CPA, CPCU**, is an internal audit manager at Western Reserve Group.

## STATEMENT OF OWNERSHIP, MANAGEMENT, & CIRCULATION

Extent and Nature of Circulation	Average No. Copies (October 2017-August 2018)	Actual No. Copies (August 2018)	Publication Title: <i>Internal Auditor</i> Publication Number: 0020-5745 Filing Date: 9-26-18 Issue Frequency: Bi-monthly Number of Issues Published Annually: 6 Annual Subscription Price: \$75.00 Mailing Address of Known Office of Publication: 1035 Greenwood Blvd., Suite 401, Lake Mary, Seminole County, FL 32746 Address of Headquarters: The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746 Contact Person: Gretchen Gorfine Telephone: 407-937-1232 Publisher: Monica Griffin, Sr. VP, CMO, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746 Editor: Anne Millage, Editor-in-chief, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746 Managing Editor: David Salierno, The Institute of Internal Auditors, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746 Owner: The Institute of Internal Auditors, Inc., 1035 Greenwood Blvd., Suite 401, Lake Mary, FL 32746 Issue Date for Circulation Data: October 2017 - August 2018 / August 2018 Signature and Title: Gretchen Gorfine, Production Manager, 9-26-18
Total Number of Copies	76,074	75,626	
Paid Circulation Mailed Outside-County Paid Subscription	58,161	58,165	
Paid Distribution Outside the Mails Including Sales, Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS	15,777	14,852	
Total Paid Distribution	73,938	73,017	
Free or Nominal Rate Copies Mailed at Other Classes Through the USPS	63	58	
Free or Nominal Rate Distribution Outside the Mail ( <i>Carriers or other means</i> )	640	649	
Total Free or Nominal Rate Distribution	703	707	
Total Distribution	74,641	73,724	
Copies Not Distributed	753	980	
Total	75,394	74,704	
Percent Paid	99.06%	99.04%	
Paid Electronic Copies	17	16	
Total Paid Print Copies + Paid Electronic Copies	73,955	73,033	
Total Print Distribution + Paid Electronic Copies	74,658	73,740	
Percent Paid - Both Print & Electronic Copies	99.06%	99.04%	



Mobile



Webinars



Online



Specialty  
Audit Centers

Ia  
INTERNAL AUDITORS  
Print



Foundation  
Partnerships



Conferences

## ENGAGE AND CONNECT GLOBALLY

**Gain a competitive edge** with unique IIA advertising and sponsorship opportunities as diverse as the 190,000 plus members from more than 170 plus countries and territories.

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

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

 **The Institute of  
Internal Auditors**





BY J. MICHAEL JACKA

## PRICE VERSUS VALUE

The only thing internal auditors should be selling is the value they provide.

You are sitting in your annual budget meeting, having provided an estimate of internal audit's expenses for the coming year. Those responsible for ensuring the appropriate use of organizational capital review your proposal with intense scrutiny. An impassioned discussion follows in which the great and powerful budget wizards look for ways to reduce spending while you argue for the resources necessary to accomplish your mission. In the heat of this battle, do you understand you are not arguing about the price of internal audit, but rather about internal audit's value?

When it comes to selling something, even internal audit's services, price is an important factor in the final buying decision. But focusing on price alone obscures the real consideration behind the buying decision—the perceived value received for that price.

Take, for example, the purchase of a diamond. Beyond issues of quality, some buyers value brand

and status. The exorbitant price of any item at Tiffany's is as much about the blue box as it is the bauble within that box. But of course not all buyers need the fancy name cachet—for some, a gem from Discount Dave's Diamonds, Dinnerware, and Dinettes will suffice.

When it comes to internal audit services, few (if any) organizations will pay the extra premium for the Tiffany's of internal audit. (This is not quite as true when it comes to external audit providers, but that is a discussion for another time.) Nonetheless, if those stakeholders have even a smidgen of understanding about internal audit, neither will they want the equivalent of a purchase from Discount Dave's.

This reality brings to mind a fundamental truth about the marketing of internal audit: The only commodity we should be selling is the value we provide. And one of the most telling moments related to the success of that sales pitch is budget time. Budget discussions can become

mercenary in nature, focusing narrowly on how much money the department will spend, how much it will be given, and how much will be taken away. And if internal audit sits in those meetings and argues price, it will almost certainly not succeed. Sure, it may win that particular battle, but it will lose the long-term war of defining and defending internal audit's value.

Budget time is the ultimate moment of truth for any internal audit department. It is when the dialogue must change. Even as other departments argue dollars and cents, internal audit must focus the dialogue on internal audit's value, followed by what the stakeholders, clients, and customers are willing to pay.

We cannot sell on being low-priced; instead, we have to sell on being the best value. [ia](#)

---

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

READ MIKE JACKA'S BLOG visit [InternalAuditor.org/mike-jacka](http://InternalAuditor.org/mike-jacka)

## DOING THE RIGHT THING

Today's boards are taking a closer look at corporate culture.



**BRIAN CHRISTENSEN**  
Executive Vice  
President - Global  
Internal Audit  
Protiviti



**TRACEY KEELE**  
Partner, Internal Audit  
and Enterprise Risk  
Services  
KPMG LLP

**In light of recent, well-publicized corporate culture failings, what are boards doing to address culture?**

**CHRISTENSEN** We definitely see the concept of culture gaining traction in the boardroom. More than ever, directors are acutely aware that culture plays a role in delivering outcomes—both good and bad—for the companies they serve. Because culture can break down anywhere in the company, it is important for directors to experience firsthand the real-world culture in the organization, rather than rely solely on boardroom discussions and management reports. One way to accomplish this is by engaging directly with operating personnel through site visits. Directors also should insist on observations regarding culture from the chief risk officer, chief compliance officer, chief information security officer, and human resources and environment, health, and

safety personnel, as well as other independent second line-of-defense functions.

Boards also expect internal audit to weigh in as the third-line assurance provider.

**KEELE** Boards are asking more directed questions: What is the risk of this happening in our company? What steps have we taken to prevent/detect this type of misconduct? Do we apply our processes consistently? How does the organization respond to a finding of inappropriate or unethical behavior—is everyone held accountable, or are certain individuals given a pass? Do we have a crisis management plan to respond to an event? Boards also should be consistently asking the broader questions that get at the current state of the organization's culture: Are expectations for what constitutes unacceptable behavior clear and understood? Is the workplace safe and respectful? Do individuals feel they can speak up without retaliation, expect

they will be heard, and have their concerns investigated?

**What do boards need to understand about their role in overseeing culture?**

**KEELE** Most boards now understand that culture is important, but determining what to do about it is another matter. Like management, boards are not entirely sure how to confirm whether the culture they want is the culture they have. Because measuring and overseeing culture isn't easy, there is a risk of defaulting to seemingly simple, check-the-box solutions. Further, there is a risk of over-relying on hard controls—policies, training, and systems that only provide a partial view of risk management. Understanding the drivers of conduct—soft controls—and whether the “walk” matches the “talk” is fundamental to understanding culture and risk.

Boards also should guard against focusing on today's expectations, without

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)

considering how they may differ tomorrow. Technological, social, economic, regulatory, and political changes are occurring faster than ever. How do organizations evolve quickly, focus on both the spirit and the letter of the law, and anticipate change to enhance resiliency, grow, and build trust with stakeholders?

**CHRISTENSEN** Culture is a vital enterprise asset that must be cultivated, nurtured, and maintained. Directors need to be curious enough to probe on culture issues. First and foremost, the board must want to know whether there are any concerns pertaining to culture warranting its attention. Board members must address two fundamental questions: How do we know what we need to know regarding culture? Is our understanding representative of the entire organization or just certain areas? No director wants to be on a board that ends up asking itself: How did this happen and why didn't we know?

#### What can internal audit do to inform the board about the organization's culture?

**CHRISTENSEN** Internal audit, the third line of defense, is well-positioned to perform a culture audit, evaluating the processes used across the entity by first- and second-line personnel to assess culture. Ironically, it is internal audit—the objective eye of the organization—that is uniquely qualified to bring “a systematic, disciplined approach” to a potentially subjective process like measuring culture. Internal auditors should “connect the dots,” considering the findings and gratuitous observations from multiple audits to ascertain whether any meaningful patterns exist. With everyone having a stake in evaluating the enterprise's culture, the board should be privy to the results of all evaluations—particularly from independent second-line functions and internal audit.

**KEELE** Internal auditors can play a critical role in understanding and enhancing culture. Internal audit can act as “the eyes and ears” of the organization, helping the board deepen its understanding of culture to better fulfill its culture oversight responsibilities. Evaluating and evolving audit skills and capabilities, initiating and promoting dialogue within the organization, garnering organizational permissions and support, and understanding the organization's culture expectations, initiatives, and current state are important first steps for establishing internal audit's role in culture.

#### What tools and techniques should internal audit use to audit culture?

**KEELE** The tools and techniques used in traditional audits also are relevant to culture audits—interviews, data review and analysis, and walk-throughs. Also, the use of surveys, facilitated workshops, focus groups, and advanced analytical techniques like sentiment analysis can be extremely valuable, deepening the understanding of employee experiences and perceptions.

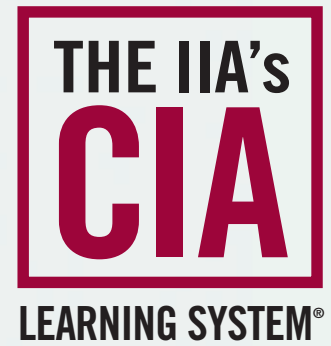
## CULTURAL MISALIGNMENT

Christensen and Keele say these red flags may indicate that the tone in the middle isn't aligned with the tone at the top.

- » Nobody is talking about culture.
- » Controversial deals and encouragement of risk taking to hit short-term targets.
- » Complex and unclear legal and reporting structures that obscure transparency.
- » Poorly executed takeovers that allow pockets of bad behavior to thrive.
- » Lack of financial discipline.
- » Employees constantly fear being fired.
- » Employees execute projects without a clear vision from company leaders.
- » Lack of knowledge sharing among employees.
- » A focus on blame or covering for each other rather than fixing the problem.
- » A perceived disconnect between words and action.
- » A focus on the letter rather than the spirit of the law and regulations.
- » Risk management and controls are regarded as an inconvenience.
- » Lack of prompt follow through on commitments.
- » Failure to escalate identified issues and active concealment of problems.
- » Dress rehearsals for leadership visits that are focused on appearance.

Internal audit should think expansively about data that exists within and outside the organization to support improved risk assessment and audit execution. Procedures should be tailored based on the organization's culture maturity and appetite for improvement, and internal audit's capability and ambition.

**CHRISTENSEN** Survey results can validate themes from stakeholder interactions to gauge consistency of views regarding the company's culture. Relevant data metrics should supplement insights from surveys and direct interactions with stakeholders. These include risk metrics, conduct-related compliance data, issue escalation and resolution data, human resources data and reports, whistleblower reports, turnover data, ethics hotline reports, unstructured social media data, and employee demographic data. These and other metrics should be used as supplements to performance measures linked to the strategy to drive the type of organizational culture that management and the board would like stakeholders to experience when they interact with it. [la](#)



# A System for Success.

Now Aligned With the 2019 CIA Exam!

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)





# IIA Calendar



## IIA CONFERENCES

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

**MARCH 11-13, 2019**  
**General Audit Management Conference**  
Gaylord Texan  
Dallas/Ft. Worth

**APRIL 29-30**  
**Leadership Academy**  
Disney's Yacht Club Resort  
Orlando

**JULY 7-10**  
**International Conference**  
Anaheim Convention Center  
Anaheim, CA

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

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

**SEPT. 16-17**  
**Financial Services Exchange**  
Washington Hilton  
Washington, DC

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

**OCT. 21-23**  
**All Star Conference**  
MGM Grand  
Las Vegas

## IIA TRAINING

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

**NEW! Auditing IT Governance**  
On Demand

**DEC. 3-12**  
**Advanced Risk-based Auditing**  
Online

**DEC. 4-5**  
**COSO Enterprise Risk Management Certificate Program**  
Dallas

**DEC. 4-7**  
**Multiple Courses**  
Orlando

**DEC. 4-13**  
**Fundamentals of IT Auditing**  
Online

**DEC. 4-13**  
**NEW! Fundamentals of Risk-based Auditing**  
Online

**DEC. 4-13**  
**Root Cause Analysis for Internal Auditors**  
Online

**DEC. 6-7**  
**COSO Enterprise Risk Management Certificate Program**  
Boston

**DEC. 10-19**  
**Performing an Effective Quality Assessment**  
Online

**DEC. 11-14**  
**Multiple Courses**  
New York

**DEC. 14**  
**Fundamentals of Internal Auditing**  
Online

**DEC. 18-19**  
**Data Analysis for Internal Auditors**  
Online

**DEC. 18-20**  
**IT General Controls**  
Online

**JAN. 7-25, 2019**  
**CIA Learning System Comprehensive Instructor-led Course – Part 1**  
Online

**JAN. 15-25**  
**NEW! Fundamentals of Risk-based Auditing**  
Online

**JAN. 22-31**  
**Audit Report Writing**  
Online

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



BY JEFFREY RIDLEY

## CREATING A BETTER SOCIETY

Internal auditors should contribute to the collective public good.

The U.K. government's recent launch of its Civil Society Strategy recognizes the social responsibility government and internal auditors have for creating the society we want to live in. Civil society in the U.K. today is not just about the well-being of the nation and everyone who lives there—it reflects the contributions we all make through our values to well-being in other civil societies across the globe. Those values are internal auditors' greatest asset and resource. They also are what internal auditing is based on and should be all about.

The strategy's aims are fourfold: Support people to play an active role in building a stronger society, unlock the full potential of the private and public sectors to support social good, help improve communities to make them better places to live and work in, and build stronger public services. I can think of no internal audit plan or program in any organization or sector that these aims and their achievement could not improve in terms of objectives, risk planning, engagement, results, findings, and follow-up.

Internal auditors all have a responsibility to make social auditing happen. Recent ventures into auditing culture and a new appreciation for culture's role in establishing effective governance practices have touched on the importance of organizational stewardship and stakeholder engagement. Culture is not just about an organization's values and how it performs. It also is about how the organization impacts the civil societies in which it operates.

Many institutional investors have signed on to the United Nations Principles of Responsible Investment with an environmental, social, and governance (ESG) duty: "To act in the best long-term interests of our beneficiaries. In this fiduciary role, we believe that [ESG] issues can affect the performance of investment portfolios." ESG as a performance measure will continue to grow in importance for governments, investors, and organizations. It should also do so for all internal auditors in every country.

Good governance embraces environmental and social responsibilities in many ways. Achievement of the U.N. Sustainable Development

Goals by its target of 2030 is just one aspect of this process. Today's responses by organizations to the development and growth of integrated and strategic reporting will have a strong influence on the future of environmental and social responsibility declarations by organizations and the assurances they give and require. Internal auditors will always have a part to play to make this happen in their own organizations, across all sectors. The U.K.'s Chartered Institute of Internal Auditors has links into voluntary networks of internal auditors working in the charity, social housing, and higher education sectors. Their messages and progress are an excellent example of how professional internal auditing is already enhancing well-being in the U.K. and across the globe. [ia](#)

**JEFFREY RIDLEY, CIA, FIIA,** is visiting professor at Birmingham City University, University of Lincoln, and London South Bank University.

*A version of this article first appeared on Audit & Risk magazine's website, [www.auditandrisk.org.uk](http://www.auditandrisk.org.uk). Reproduced with permission.*

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



# Make 2019 Your Best Year Yet

Closing this year's audit plan is the optimal time to reevaluate processes and tools that may be slowing you down.

Wdesk for Internal Audit Management is a streamlined, collaborative platform that saves you valuable time. Focus on strategic areas that position you for success in the months—and years—to come.

See how Wdesk works at [workiva.com/IIA-video](https://workiva.com/IIA-video)

**workiva**<sup>®</sup>



# A VIBE ALL ITS OWN

The IIA's **2019 International Conference** is coming to Southern California.

Registration now open. [ic.globaliia.org](http://ic.globaliia.org)

 THE INSTITUTE OF INTERNAL AUDITORS  
**INTERNATIONAL  
CONFERENCE**  
SOUTHERN CALIFORNIA, USA / 7-10 JULY 2019

