

# Ia

INTERNAL AUDITOR

APRIL 2020

A PUBLICATION OF THE IIA

Road Testing RPA

Beyond Third Parties: Auditing  
the Business Ecosystem

Assessing Knowledge Asset Risks

10 FAQs About  
Organizational Culture

## THE RESPONSIBLE ORGANIZATION

Internal audit needs to consider the value proposition around ESG  
and push the business case for change.





# Featuring

## *Internal Auditor Blogs*

*Voices with viewpoints on the profession*

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

### **Chambers on the Profession:**

Seasoned Reflections on Relevant Issues

### **From the Mind of Jacka:**

Creative Thinking for Times of Change

### **Solutions by Soileau:**

Advice for Daily Audit Challenges

### **Points of View by Pelletier:**

Insights and Innovations From an Insider

**READ ALL OF OUR BLOGS.** Visit [InternalAuditor.org](http://InternalAuditor.org).

**la**  
INTERNAL AUDITOR



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

Assure. Advise. Anticipate.

As organizations push the bounds of disruption, the role of the internal audit function needs to evolve to not only deliver assurance to stakeholders, but to advise on critical business issues and better anticipate risk. Through custom labs, we can help you develop a strategy to modernize your internal audit program, tapping into the power of analytics and process automation; identifying and developing the skills and capabilities required to build and sustain the internal audit function of the future; and incorporating Agile internal audit to keep up with the rapid pace of change. The future is now.

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



# FAILURE

*to make the grade*

## AMERICAN CORPORATE GOVERNANCE INDEX

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



**Download your free copy today.**

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





## F E A T U R E S

**26 COVER The Responsible Organization** As investors focus on ESG reporting, there is opportunity for internal auditors to get involved and provide assurance. **BY NEIL HODGE**

**32 An RPA Road Test** Internal auditors at a freight transportation company take robotic process automation for a test drive. **BY RICK WRIGHT**

**39 Audit With Acumen** Internal audit can incorporate elements of the Balanced Scorecard approach to build its ability to anticipate and meet the organization's needs. **BY BASIL ORSINI**

**44 The Value in the Business Ecosystem** Internal audits must delve into risks posed by the organization's ever-expanding

chain of third, fourth, and fifth parties.  
**BY BRIAN KOSTEK**

**50 10 Questions on Culture** Several audit committee FAQs can help guide practitioners when assessing culture. **BY PETER HUGHES, ROBERT CAMPBELL, AND JOHN LERIAS**

**54 Auditing Knowledge Management** Knowledge assets' increased value and contribution to business objectives obliges internal auditors to focus on how they're safeguarded.  
**BY ISRAEL SADU**



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



*be* instrumental

## Donations Are Instrumental to Innovation

Generous contributions are instrumental for the Internal Audit Foundation to conduct groundbreaking research, publish invaluable thought leadership, and forge new partnerships to elevate the profession.

For more than 40 years, the Foundation has served the internal audit profession by:

- Delivering timely tools and research to help boost career growth.
- Providing educational products to empower internal auditors.
- Filling the employment pipeline with qualified candidates.

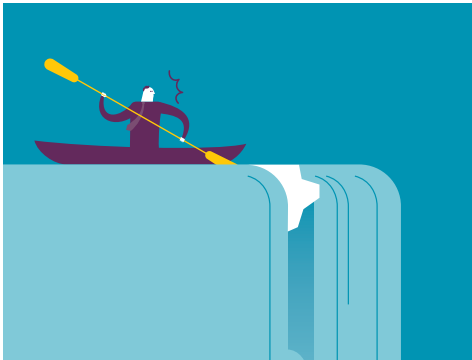
Help us orchestrate internal audit innovation by making your tax-deductible donation.

---

**Support Your Foundation.** [www.theiia.org/Foundation](http://www.theiia.org/Foundation)



## DEPARTMENTS



**7 Editor's Note**

**8 Reader Forum**

**67 Calendar**

### PRACTICES

**10 Update** Audit plans miss key risks; boards fall short on diversity; and human error is behind most data breaches.

**14 Back to Basics** Internal audit plays a role in developing fraud policy.

**17 ITAudit** Benford's Law can detect anomalies better than traditional techniques.

**20 Risk Watch** Some organizations have an irrational aversion to risk.

**23 Fraud Findings** An employee tip reveals a multimillion-dollar T&E scam.

### INSIGHTS

**60 Board Perspectives** Internal audit can help assure a smooth process to handle CAMs.

**63 The Mind of Jacka** Auditors looking to succeed would do well to follow three rules.

**64 Eye on Business** Cloud computing solutions come with challenges.

**68 In My Opinion** Boards sometimes have split priorities.

## ONLINE [InternalAuditor.org](https://www.internalauditor.org)



**My First Audit Committee Meeting** A veteran practitioner shares lessons learned from his first time in the hot seat fielding questions from committee members.

**Auditing Culture: Familiar Techniques** There's no need for a radically different approach – tried and true methods can go a long way on culture audits.

**Balancing Transformation With Security** Boards, business units, and cybersecurity functions aren't all on the same page about protecting the organization's digital initiatives.

**Building Scheme Is No Big Hit** A businessman allegedly used restaurant licensing deals with country music stars as a lure to defraud U.S. construction developers.



# EMERGING LEADERS 2020

## Who Are Internal Auditing's 2020 Emerging Leaders?

### What defines an extraordinary internal auditor?

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

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

Nominate by May 18, 2020 at [www.InternalAuditor.org](http://www.InternalAuditor.org).







## THE RESPONSIBLE INTERNAL AUDITOR

**D**o you know a young internal auditor who is making a difference? Since 2013, *Internal Auditor* has been recognizing up-and-coming auditors from around the world who are advancing the profession in our annual “Emerging Leaders” article.

How are they making a difference? The internal audit professionals chosen to be Emerging Leaders rise to the top based on their business acumen/leadership skills, innovative thinking, community service, and service to the profession. These well-rounded individuals care about their communities, understand their organizations, and are always looking for new and better ways to do their jobs—three areas of focus in this issue.

Our cover story, “The Responsible Organization” (page 26), considers internal audit’s role in environmental, social, and governance (ESG) reporting. Paul Sobel, chair of The Committee of Sponsoring Organizations of the Treadway Commission, says internal audit needs to consider the value proposition around sustainability. “Internal audit needs to look at what future investor, regulatory, and stakeholder expectations are likely to be regarding sustainability risk management and reporting and push for management and the board to move in line—or ahead—of them,” he says.

Every year, a common trait of our Emerging Leaders is their understanding of the importance of innovation in their organizations and in their departments. In “An RPA Road Test” (page 32), author Rick Wright takes readers through a pilot robotic process automation (RPA) program at his company, YRC Worldwide. “Audit leadership saw RPA’s potential ... as a critical piece of internal audit’s strategy,” Wright says. “Automating portions of the standard terminal audit program could free up valuable staff resources, allowing more focus on other value-added services.”

Finally, in this issue, we tackle the important topic of business acumen, an area in which Emerging Leaders excel. In “Audit With Acumen” (page 39), author Basil Orsini offers four examples of business acumen in internal audit based on perspectives adapted from the Balanced Scorecard strategic planning and management tool. He writes, “Internal audit can build business acumen on a sound understanding and innovative implementation of the *Standards* and associated guidance.”

As your internal audit team’s expertise grows in the areas of ESG, innovative thinking, and business acumen, who stands out? Now is the time to nominate them for *Internal Auditor* magazine’s 2020 Emerging Leaders and give them the recognition they deserve. Visit [InternalAuditor.org](http://InternalAuditor.org) to make your nomination. Nominations are open through May 18.



@AMillage on Twitter

## Reader Forum

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



**Correction:** In Louis Seabrooke and Amy Felix's "A Study in Risk Tolerance" (February 2020) there was an error in the chart, "The Risk Tolerance Model" that affected the scoring system. The corrected chart appears at [www.theiia.org/AStudyInRiskTolerance](http://www.theiia.org/AStudyInRiskTolerance).

### Regulatory Blueprint

Nancy Haig's article was excellent in laying out the blueprint for organizations adapting to regulatory changes that affect operations. This information should be printed on posters and cards to give senior management when



dealing with changes or on how to resolve audit recommendations. The article was straightforward and the example was on point to follow. Auditors could use this information to provide valuable information to senior management of their organizations.

**FREDRICK W. LEE** comments on Nancy Haig's "A Plan for Regulatory Change" (February 2020).

### AI's Inherent Bias

One of the key risks is related to ethical bias of artificial intelligence (AI) in making a decision based on a competing set of objectives or defining the objectives too narrowly without balancing the needs of other stakeholders and affected parties. Problems may also arise on the usage of data that has inherent biases such as facial recognition algorithms using images or information skewed toward or against a certain race or gender.

Internal auditors would need to focus on these inherent risks in the design of AI/machine learning algorithms in design and data governance,

and provide assurance around controls that mitigate these risks.

**UDAY GULVADI** comments on Kevin Alvero and Wade Cassels' "Bringing Clarity to the Foggy World of AI" (February 2020).

### Doing What You Love

What Mike Jacka describes is largely why I left my last job—it was all about templates, checklists, forms over substance, etc. It reminds me of playing the game Operation, where if you veer 1 millimeter this way or that, "Buzzz!" and you lose.

With my new company, there's room to learn, explore, try, ask, challenge, and be—heaven forbid—creative. I want to thank Jacka for helping me to clarify my feelings and give me a shot in the arm to keep trying and doing what I love—improving organizations.

**SEAN BORZEA** comments on Mike Jacka's "Drunk and in Charge of a Bicycle" ("The Mind of Jacka," February 2020).



**VISIT [InternalAuditor.org](http://InternalAuditor.org) to comment on the latest articles.**

**Ia**  
INTERNAL  
AUDITOR

APRIL 2020  
VOLUME LXXVII:II

**EDITOR IN CHIEF**  
Anne Millage

**MANAGING EDITOR**  
David Salierno

**ASSOCIATE MANAGING EDITOR**  
Tim McCollum

**SENIOR EDITOR**  
Shannon Steffee

**ART DIRECTION**  
Carol Hardy Design

**PRODUCTION MANAGER**  
Gretchen Gorfine

#### CONTRIBUTING EDITORS

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

#### EDITORIAL ADVISORY BOARD

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

J. Michael Jacka, CIA, CPCU, CFE, CPA  
Sandra Kasahara, CIA, CPA  
Michael Levy, CIA, CRMA, CISA, CISSP

Merek Lipson, CIA  
Michael Marinaccio, CIA  
Alyssa G. Martin, CPA  
Joe Martins, CIA, CRMA  
Stephen Minder, CIA  
Rick Neisser, CIA, CISA, CLU, CPCU  
Hans Nieuwlands, CIA, RA, CCSA, CGAP  
Manish Pathak, CA  
Bryant Richards, CIA, CRMA  
James Roth, PhD, CIA, CCSA  
Jerry Strawser, PhD, CPA  
Glenn Summers, PhD, CIA, CPA, CRMA  
Robert Taft, CIA, CCSA, CRMA  
Brandon Tanous, CIA, CGAP, CRMA  
Stephen Tiley, CIA  
Robert Venzel, CIA, CRMA, CISA  
David Weiss, CIA  
Rick Wright, CIA

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

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

#### CONTACT INFORMATION

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

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

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

**PERMISSIONS AND REPRINTS**  
[editor@theiia.org](mailto:editor@theiia.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.

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





## IIA Training Stations

IIA ONDEMAND

# Learn From The Leader.

IIA TRAINING ONDEMAND  
PLATFORM OPEN 24/7

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

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


 The Institute of  
Internal Auditors

Boards fall short on ethnic diversity... Insider actions lead to data breaches... Audit's role in a pandemic... Email fraud targets CEOs and employees.


# Update


## THE STATE OF AI


U.S. technology company decision-makers have high hopes and some concerns for artificial intelligence.

**88%**   
Companies should implement an ethics policy to govern their AI work.

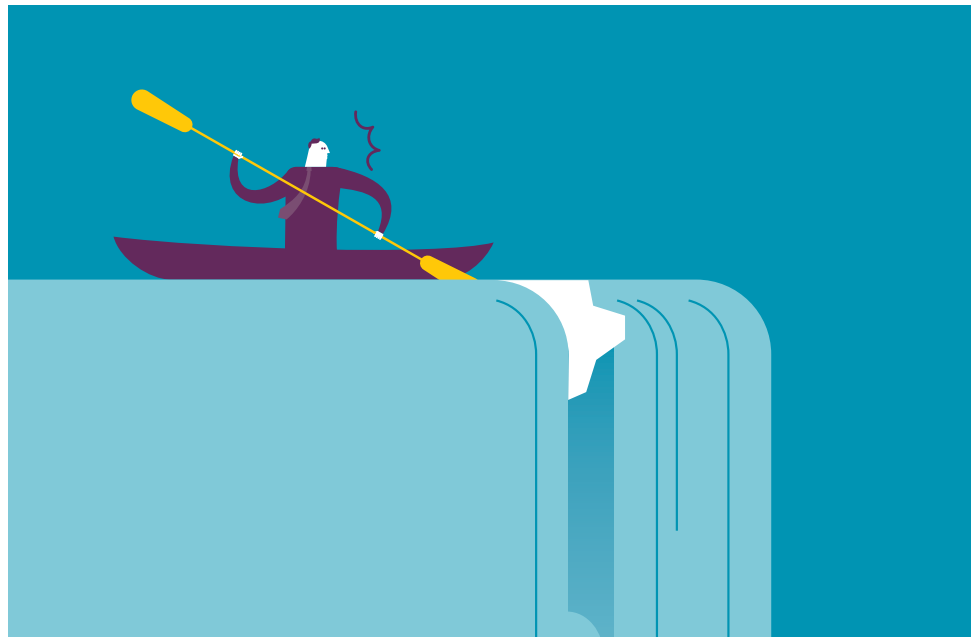
 **69%**  
Governments should regulate AI.

**62%**   
AI adoption is moving at an appropriate speed across the technology industry.

 **61%**  
Existing employees are prepared for AI adoption.

**37%**   
AI could replace their positions.

Source: KPMG, Living in an AI World 2020 Report: Technology Insiders



## AUDIT PLANS IGNORE KEY RISKS

Internal audit departments are leaving key risks out of their audit plans, The IIA's 2020 North American Pulse of Internal Audit reports. The survey of 630 chief audit executives, directors, and managers reveals a glaring disconnect between high risks and audit priorities.

Take cybersecurity, rated a high risk by more than three-fourths of respondents. Cybersecurity is the Pulse's top risk, yet almost one-third say it's not included in the internal audit plan. Another disconnect is third-party relationships—more than half of respondents rate it a high risk, but less than half include it in the audit plan.

Cybersecurity and third parties are among omissions, Pulse says.

Then there is sustainability risk, which only 10% include in their audit plan. Although only 6% of respondents rate sustainability a high risk, there is growing investor interest in it (see "The Responsible Organization" on page 26). That also was the case for another rising investor priority—governance and culture—which less than half of respondents include in their audit plan.

Such shortfalls in risk coverage were noted in The IIA's OnRisk 2020 and American Corporate Governance Index studies, says IIA President and CEO Richard Chambers. "The Pulse shows just how serious the

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

IMAGES: TOP, AKINDO / ISTOCKPHOTO.COM;  
LEFT, VENOMOUS VECTOR / SHUTTERSTOCK.COM



problem is, and its impact on sustainability, operational efficiency, and culture,” he says.

In addition to missing top risks, one in five are performing below the midpoint (level 3) of the Internal Audit Ambition Model, a maturity scale developed by IIA–Netherlands and LKO/NBA. Those functions aren’t conforming with the *International Standards for the Professional Practice of Internal Auditing*.

The good news is more than half of respondents say their department is performing at the top two levels of the five-level model. Twelve percent rate themselves at the top level (Optimizing), while 40% are at Level 4 (Managed). Such functions support strategic risk management, long-term planning, and continuous improvement.

—T. MCCOLLUM

## BOARDS FALL SHORT ON DIVERSITY EFFORTS

A U.K. report shows failure to prioritize board ethnicity.

**F**ewer than half of Financial Times Stock Exchange (FTSE) 250 companies mention ethnicity in their board diversity policy, according to research from the U.K.’s Financial Reporting Council (FRC) and Cranfield University’s School of Management. The report, *Ethnic Diversity Enriching Business Leadership*, also shows that most of the broader FTSE 350 lacks measurable ethnicity targets.

Only 14% of FTSE 100 companies—the U.K.’s largest publicly listed firms—set measurable objectives for board ethnic diversity; the proportion drops to 2% for the FTSE 250. Even where objectives are established, FTSE 350 companies have not made progress against them. The research also finds that while just over 10% of FTSE 100 firms plan to increase ethnic



diversity in succession planning, most of these firms emphasize progression companywide, rather than at the top.

In light of the FRC’s report, the 2020 Parker Review, an independent report on the ethnic diversity of U.K. boards, recommends companies report on diversity of culture, geography, and nationality alongside ethnicity. —D. SALIERNO

## INSIDER THREATS PUT DATA AT RISK

Human error is behind most data breaches, research says.

**T**hree-fourths of IT professionals say employees at their organizations have intentionally put data at risk in the last 12 months, according to research conducted by Opinion Matters

for Egress, a data security solutions company.

Additionally, 78% say employees have accidentally done so. These insider threats pose a significant security risk to organizations, Egress reports.

The Insider Data Breach Survey 2020 polled more than 500 IT leaders and 5,000 employees at companies with more than 100 employees in Belgium, Luxembourg, Netherlands, the U.K., and U.S. It found that



**THE IMPACTS FROM CLIMATE CHANGE AND LOSS OF NATURE COULD COST THE GLOBAL ECONOMY**

**\$9.87**

trillion between now and 2050.

**THE ECONOMY COULD LOSE**

**\$327**

billion from damage to natural protections from flooding, storm surges, and erosion, while loss of carbon storage could cost \$128 billion by 2050.

“Not only will losing nature have a huge impact on human life and livelihoods, it will be catastrophic for our future prosperity,” says Marco Lambertini, director general of WWF International.

Source: WWF, Global Trade Analysis Project, and the Natural Capital Project, Global Futures



# An Exclusive Opportunity

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

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

## 2020 VISION UNIVERSITY SESSIONS EXECUTIVE DEVELOPMENT

---

### Boston, MA

June 15–18  
Omni Parker House

### San Diego, CA

Sept. 14–17  
Kimpton Solamar Hotel

### Chicago, IL

Nov. 2–5  
Kimpton Hotel Palomar

---

*Your CAE Success Story Starts Here*

VISION UNIVERSITY



AUDIT EXECUTIVE  
CENTER

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



41% of employees who have accidentally leaked information did so because of phishing emails. Nearly one-third caused a breach by sending an email to the wrong person, and almost half have received an email recalling information sent in error.

Egress CEO Tony Pepper explains that organizations and their security teams weigh the advantages of efficient communications against data security considerations. “Frequently they compromise on the latter,” he says.

Employee misconceptions about data ownership negatively impact information security, the survey shows. Two out of five employees don’t recognize that the organization owns its data exclusively, and only 37% say everyone is equally responsible for keeping it safe. “Employees want to own the data they create and work on, but don’t want the responsibility for keeping it safe,” Pepper says. “This is a toxic combination for data protection efforts.”

The more senior the employee, the less likely he or she is to accept data protection accountability liability—just 8% of directors say everyone shares responsibility, compared to more than half of clerical staff. Directors also are most likely to take data with them to a new job. Of those who intentionally broke company policy, 68% did so when they changed jobs, compared to the overall average of 46%. —**S. STEFFEE**

## THE PRESSURE OF PANDEMICS

During an outbreak, internal audit should focus on stronger controls, says Business Continuity Management Institute President Moh Heng Goh.



**How can internal audit functions support business continuity during pandemics?** Once a pandemic like the coronavirus (COVID-19) has occurred, there is little an auditor can be involved in as major audit activities should be reduced due to the possibility of transferring infection between auditor and client. Additionally, the client’s focus may be on the response and recovery of its critical business functions.

While the outbreak is occurring, the audit team can focus on possible breakdowns in controls of processes as business functions operate from a remote or alternate location, or even from home. The key is to strengthen the controls to minimize the potential for errors resulting from manual interventions and the possibility of fraud. It is important to note that the observance of noncompliance with existing protocols should be based on its materiality so that the organization can respond and recover in the shortest possible time.

Business continuity plan reviews are typically predetermined by a business continuity management policy. The frequency of review and updating is usually annual. During a pandemic, like any other disruption, these reviews may need to be conducted more frequently when an audit client’s environment has frequent staff turnover, or if outsourcing or transferring business functions to a third party results in an interdependency risk.

## NO. 1 CYBERCRIME: EMAIL FRAUD

Hackers target company employees in record numbers.

Business email compromise accounted for more than half of total reported U.S. cybercrime last year, according to the Federal Bureau of Investigation’s (FBI’s) 2019 Internet Crime Report. These scams, which typically involve a criminal mimicking a legitimate email address, resulted in more than \$1.7 billion in losses in 2019. They were responsible for nearly 24,000 complaints made to the FBI’s Internet Crime Complaint Center (IC3) last year.

Many compromised emails are CEO fraud, where an email sender impersonates an executive within the company. The email requests payment that appears legitimate but actually directs funds to a criminal.

IC3 also reports an increase in complaints that involved diversion of payroll,



where hackers mimic an employee requesting an update to his or her direct deposit information. The change then routes that employee’s paycheck to a scammer’s account.

Last year saw the largest number of cybercrime complaints since 2000. —**D. SALIERNO**

# Back to Basics

BY CHRIS ERRINGTON, MICHELE NISI + KEVIN M. ALVERO

EDITED BY JAMES ROTH + WADE CASSELS

## BREAKING DOWN THE FRAUD POLICY

Internal auditors need to be involved in, and understand, the organization's fraud detection and prevention efforts.

Nearly half of all global organizations in PwC's 2018 Global Economic Crime and Fraud Survey admit to having been the victim of fraud and economic crime in the past two years, resulting in more than \$7 billion in total losses and a median loss of \$130,000 per case. Nearly half of those frauds were because of internal control weaknesses.

Internal audit plays several key roles in the prevention, detection, and monitoring of fraud risks. First, as internal audit has broad visibility into the different areas of the enterprise, it should be aware of potential red flags of fraud in all audit engagements and identify ones that may warrant further investigation. Also, internal audit should assess the effectiveness of controls designed to mitigate fraud risk. Finally, internal audit can lend valuable expertise in an advisory role to the development of the fraud policy.

To do this, internal auditors need to understand the key elements of a strong policy, and who it should involve.

### The Building Blocks

Any organization can be a victim of fraud, regardless of its size, industry, or location. The most effective recourse is to develop a strong and implementable fraud policy that defines unacceptable behavior and how the organization will respond to it. While policies can vary depending on the organization's number of employees, industry complexity, and operating environment, the fundamental elements remain the same:

- The policy has top-down support.
- It includes clear, specific language and examples.
- It accurately and effectively defines fraud.
- There is policy ownership, so a specific person or group of people are charged with overseeing

the development and implementation of the fraud policy.

- It clearly spells out personnel roles and responsibilities.
- It explains the disciplinary and legal actions the organization will take.
- It makes anonymous hotlines and reporting options available.
- There is an effective communication plan around the policy.

While no fraud policy can define every fraudulent action, a well-written policy uses clear language and relatable examples to help reduce uncertainty of what the organization considers illegal activity. It also provides clear instructions regarding the responsibilities and procedures to be followed by all involved when illegal activity is suspected or uncovered.

However, it doesn't matter how well the fraud policy is written if it sits in a three-ring binder gathering dust. The organization must

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

ensure that the fraud policy is not only created, but also read and understood by all internal personnel and external parties with which it engages. The greater the importance the organization places on this document, the greater the likelihood employees will place an equal amount of importance to it. From regular manager/employee policy reviews to live training to role playing, the same message, stance, and emphasis on eliminating fraud can be reinforced. Regular communication not only promotes understanding, but also can deter potential fraudsters.

Occupational fraud is most efficiently organized into three categories, each of which companies must identify and communicate with personnel.

- ➔ *Asset misappropriation* is the stealing or misuse of enterprise resources by personnel. This occurred in more than 89% of all reported cases and resulted in a median loss of \$114,000, according to the Association of Certified Fraud Examiner's (ACFE's) Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse.
- ➔ *Corruption schemes* occur when personnel misuse their influence during business transactions to obtain benefit and violate their duties to the employer. According to the ACFE study, this results in 38% of occupational fraud cases with a median loss of \$250,000.

## It's critical that the fraud policy conveys a plan of disciplinary action.

- ➔ *Financial statement fraud* occurs when personnel intentionally cause misstatements or omit information in enterprise financial reports. It is the least common but most costly, averaging \$800,000 per incident.

### Prosecuting Fraud

While fraud detection and prevention is an organizationwide effort, clearly defined roles must be instituted to promote responsibility and reduce confusion. For example, the board of directors is responsible for corporate fraud governance, and management must be engaged in executing these policies. Internal audit's role should be clearly defined, as well. Auditors must have the authority to ensure fraud controls are appropriate and effective, to investigate instances of possible fraud, and to support management in executing the fraud risk assessment.

Without the threat of prosecution, a fraud policy is little more than a toothless tiger. Therefore, it's critical that the policy conveys a plan of disciplinary action to all personnel.


The fraud policy must include a statement that all appropriate measures to deter fraud will be taken and all instances of suspected fraud will be investigated and reported to the appropriate authorities.

Generally, organizations have four options when fraud is uncovered: criminal prosecution, civil fraud lawsuit, a mutually agreed upon termination of the perpetrator, or no action. There are varying schools of thought as to which of these actions should apply to different fraud situations. For example, it can be argued that taking no action is one of the surest ways to promote an organization's susceptibility to future fraud because of the perception of impunity. On the other hand, there also are cases when the cost of prosecution exceeds the cost of the fraud and other disciplinary actions may be preferred. Some organizations will prosecute all fraud regardless of monetary value. From the internal auditor's perspective, however, the key question is whether the organization has considered the risks of its disciplinary policy (reputational risk, cost, future fraud risk, etc.) and is comfortable with them.

The fraud policy must provide personnel with instructions regarding the steps to take when suspecting fraud. The policy should remind personnel that they are not prosecutors of the law and that their job is to report their findings to the organization's appropriate party. The fraud policy should provide anonymous avenues to give employees confidence that they can safely report potential fraud, such as a fraud hotline number. In addition to verifying the existence of a hotline,

internal audit also may want to understand whether it is being used and how effectively the company has responded to these tips.

### A Preventive Measure

In the end, a fraud policy is an inexpensive and effective method for reducing the threat of potentially crippling financial losses. Furthermore, all departments, including internal audit, can play major roles in its development. This stand-alone document should be seen by all personnel as playing an integral role in the organization's health and longevity. 

**CHRIS ERRINGTON, CRCMP, CSPO, GRCP**, is a senior communications specialist in the Internal Audit department at Nielsen in Oldsmar, Fla.

**MICHELE NISI, CIA, CFE, CPA**, is a manager in the Internal Audit department at Nielsen.

**KEVIN M. ALVERO, CISA, CFE**, is senior vice president, Internal Audit, Compliance, and Governance, at Nielsen.

Internal Audit, Risk, Business & Technology Consulting

# Illuminating the Top Global Risks in 2020

Explore Protiviti's digital Executive Perspectives on Top Risks 2020 report and prepare for the risks likely to affect your organization this year.



Visit [protiviti.com/toprisks](https://protiviti.com/toprisks) for the full report.

[protiviti.com](https://protiviti.com)

protiviti®  
*Face the Future with Confidence*

## BENFORD'S LAW IN A BIG DATA WORLD

Applying the mathematical digital analysis tool to large data sets can help auditors detect fraud and other problems.

The power of Benford's Law has never been as critical given the rise of big data and computing power. The digital analysis tool has been used in numerous high-profile forensic investigations, including investigations of voter fraud in the 2009 Iranian election and Greece's efforts to hide its debt in 2015.

A Benford's Law review of 5,400 contracts at a Canadian nonprofit organization found the numeral "4" as the first digit 16% of the time, compared to the expected 9.7%. That finding enabled the internal auditor to uncover questionable contracts in amounts between \$40,000 and \$49,999 that totaled \$15 million. Those contracts were approved by an employee who directed them to vendors who were his associates.

In addition to detecting fraud, internal auditors can use Benford's Law to identify inefficient processes and computer bugs.

It does this by determining the expected frequency for any digit in a set of discrete numbers such as journal entries, disbursements, and revenues. This means that a digit in a number in a given data set is mathematically predictable. Because the expected frequency for each digit is known, every item in excess of that frequency is deemed unusual.

With large amounts of data to analyze, Benford's Law can detect anomalies better than traditional audit techniques. For example, research shows that companies whose financial statements are significantly out of compliance with Benford's Law are likely to get caught for accounting irregularities. A before-and-after comparison of restated earnings showed that the new, real numbers aligned with Benford analysis.

Internal auditors can leverage audit software with Benford's Law functionality. Additionally, some audit

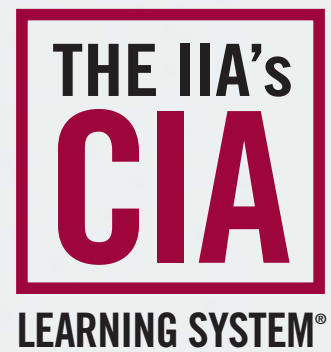
departments can work with the organization's IT function to adopt a step-by-step Benford analysis using established formulas to analyze company data for unusual patterns.

### Revealing Fraud

Because few fraudsters know about Benford's Law, the numbers they cook up stand out. As a result, the position of each digit in their transactions will not follow Benford's analysis, revealing their crime (see "Benford's Basics" on page 19).

For example, during a purchasing audit at a retail company, internal auditors discovered there were 550 purchase orders issued with the first two digits "96," compared with the expected count of 289 purchase orders. Benford's Law analysis showed 145 purchase orders of between \$9,600 and \$9,690 were approved by a director whose approval authority was limited to \$10,000. Further investigation revealed that over a





# A System for Success.

Prepare with Confidence & Convenience.

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



Prepare to Pass. [www.LearnCIA.com](http://www.LearnCIA.com)





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

## BENFORD'S BASICS

**B**enford's Law made its debut in the audit profession in the 1990s through the efforts of Mark Nigrini, an expert on the theory. First discovered in 1881 by mathematician Simon Newcomb, the theory lay dormant for almost half a century until the 1930s when it was again discovered by physicist Frank Benford.

Benford determined that leading digits are distributed in a specific, nonuniform way. This discovery led to the mathematical theory that in large sets of data, the initial digits of amounts will tend to follow a predictable pattern. The initial digit "1" is most common as the first

digit in data sets, appearing 30% of the time, followed by "2" (17.6%), "3" (12.5%), "4" (9.6%), "5" (7.9%), "6" (6.6%), "7" (5.8%), and "8" (5.1%). The initial digit "9" appears the least often (less than 5%).

Benford's Law works because the distance from "1" to "2" is far greater than the distance from "9" to "10." For example, if a data set begins with the digit "1," it has to increase by 100% before it begins with the digit "2." To get from "2" to "3" requires a 50% increase; from "3" to "4," 33%; "4" to "5," 25%; "5" to "6," 20%; "6" to "7," 16%; "7" to "8," 14%; "8" to "9," 12%; and "9" to "10," 11%.

two-year period, the director made \$3.5 million in purchases for personal items such as electronics, jewelry, and appliances.

### Five Types of Analysis

Basic tests in Benford's Law cover first-digit analysis, second-digit analysis, first two-digit analysis, first three-digit analysis, and last two-digit analysis.

- » **First-digit Analysis** Auditors can chart the expected and actual occurrence for each digit from "1" to "9." They can drill down further on unusual differences for analysis and action.
- » **Second-digit Analysis** Like the first-digit analysis, the second-digit analysis is a test of reasonableness. At a health-care company, an analysis of the second digits in more than 21,000 payroll records revealed that the numeral "0" turned up as the second digit twice as often as it should have. The numeral "5" showed up 60% more often than expected. Based on those findings, the records were deemed fraudulent.
- » **First Two-digit Analysis (F2D)** There are 90 possible combinations (10 through 99) for the first two digits in a number. For example, the first two digits of 110,364 are "11." In an F2D test, Benford's Law would note there is a 3.8% likelihood that "11" would be the first two digits. This is a much more focused test as the purchase order example showed.
- » **First Three-digit Analysis (F3D)** In F3D tests, there are 900 possible combinations (100 through 999), allowing for an in-depth analysis of large data sets. It provides greater precision for picking up abnormal duplications in sets with 10,000 or more transactions.
- » **Last Two-digit Analysis** There are 100 possible combinations (00 through 99) in the last two digits

of a number. The expected proportion for each of these combinations is 1%. Any excess is rounded off or are invented numbers.

### When to Use It

Benford's analysis is best used on data sets with 1,000 or more records that include numbers with at least four digits. As the data set increases in size, closer conformity to the expected frequencies increases.

However, not all financial data lend themselves to such tests. Benford's analysis cannot be used in scenarios such as:

- » A data set made up of assigned numbers such as Social Security, contract, invoice, phone, customer, and check numbers.
- » Psychological thresholds such as \$199.99.
- » Minimum and maximum numbers such as a petty-cash fund disbursing between a \$10 minimum and a \$40 maximum.
- » Where no transaction is recorded such as thefts, kickbacks, and contract rigging.
- » Limiting a sample of transactions to only between a narrow range, such as between \$100 and \$999.

### Extract Needles From Digital Haystacks

Benford's Law can be a powerful way to combat the costly scourge of fraud. It is like placing a magnet over a haystack and extracting the needles, enabling internal auditors to analyze an entire population of data. All it takes is an interest and a willingness to learn new approaches. [la](#)

**LAL BALKARAN, CIA, FCPA, FCGA, FCMA**, is an internal auditor and independent consultant with more than 30 years' experience based in Scarborough, Ontario.

# Risk Watch

BY RICK WRIGHT

## A RATIONAL MINDSET

Risks, like snakes, are often viewed as threats, despite their potential benefits.

Remember the scene from *Raiders of the Lost Ark* where Indiana Jones enters the Well of the Souls, which happens to be a snake-infested pit? After throwing a torch into the pit to reveal his plight, he exclaims, “Snakes ... why did it have to be snakes?”

Granted, this scene is plotted to presume the snakes are venomous, so Indiana’s fear is rational. But his initial reaction reveals his bias about snakes in general—the same way some people are irrationally averse to risk.

Internal auditors have a professional duty to remain objective as they perform their work. This unbiased mindset must extend to remaining rational when it comes to communicating with audit clients about risk.

### Why Did It Have to Be Risk?

Snakes are vilified as animals that hide in dark places, stealthily seeking out

prey and striking when they least expect it. An objective study of snakes reveals a much more accurate view of these complex creatures. Not all snakes are aggressive, nor are they all venomous or massive constrictors capable of inflicting great harm to people, as we often see in movies or hear about in the news.

In fact, snakes can be beneficial. Take the black rat snake, which is effective at controlling harmful rodent populations. One black rat snake can eat 100 mice per acre in a year. What farmer wouldn’t readily adopt at least a couple of these hunters to offset the negative impact mice have on property and equipment, not to mention the potential spread of disease?

People sometimes perceive risk with the same irrational viewpoint. Too often, when discussing risk and risk management philosophy with business professionals in the course

of internal audit work, the conversation gravitates toward an unbalanced, negative attitude about risk.

One time, my audit team was conducting an audit workshop with a group of business managers. The team was explaining how our audit activities were risk-based so that we focused on things that matter most to their functions’ success. The supervisor for this group of managers interrupted our discussion to admonish the group that they needed to be focused on risk to eliminate it from the company. While it was an innocent exclamation the supervisor truly believed, it was an unfortunate and unplanned distraction from our discussion that the audit team had to clarify with the workshop participants.

The interruption turned out to be a blessing in disguise. It enabled the internal audit team to lead a healthy discussion about

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





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

the opportunities that also accompany risk, while explaining that eliminating risk was not realistic nor necessarily a desirable goal.

### Shifting the Risk Mindset

With all the focus organizations have devoted to enterprise risk management and updated risk management frameworks, they still get trapped in a vortex where risk is seen in a lopsidedly negative light. Internal audit should thoughtfully redirect this line of thinking when such an uninformed view of risk and risk management is expressed.

The snake analogy is a good proxy for reframing the risk discussion. The word *risk* often is misunderstood. Like snakes, risk can do serious harm, so people instinctively project harm to all risk. But is this rational?

In finance, *risk* frequently is paired with the word *reward* to describe offsetting outcomes related to a decision. While taking any given risk may result in a bad outcome, there also is the prospect of a good outcome. No risk, no reward, as the saying goes. This is a more rational view of risk.

Internal auditors can help organizations balance attitudes about risk by talking and acting rationally about risk. For instance, they shouldn't use risk exclusively as a

stakeholders are more likely to respond to risk with a more rational mindset.

### Thinking Differently About Risk

Let's think about snakes and risk a little differently. A more neutral word to use for snake is reptile. Some reptiles can cause harm to people in certain circumstances such as swimming in a lake known to have large alligators or walking through terrain known for rattlesnakes. In other situations, such as rodent control, reptiles are benign or helpful.

Likewise, a less polarizing term for risk is uncertainty—specifically, about some outcome. Risk is neither bad nor good; it's just uncertainty. When auditors use the word *uncertainty* when discussing risk, they can have a more objective, and less polarized, discussion and avoid the biased, negative connotation. This allows auditors to unlock the real value of an intellectual discussion about risk—refocusing attention on decision-making.

Uncertainty hinders decision-making. The more uncertainty that exists about a pending decision, the more difficult it is to make a decision that will result in a favorable outcome. The better decision-makers can understand the uncertainty they are faced with in a decision, the more likely they should be able to optimize the outcome they are seeking from any given decision.

The coronavirus pandemic comes to mind. In the present, fear of the unknown is dominating the response conversation. This is a crisis that has not been experienced in most of the modern world, and government leaders are struggling to craft effective responses

**The more uncertainty that exists, the more difficult it is to make a decision that will result in a positive outcome.**

“four-letter word” in discussions with other business professionals. Risk mitigation is only one potential risk response alternative. When approaching risk assessments or new audit engagements, internal auditors should talk about how informed risk-taking is essential to the organization's growth prospects.


Internal auditors should counsel clients that risk acceptance is sometimes the best risk response. This can be the case when other risk response alternatives are costly or when the risk is relatively mild. Accepting a risk while continuing to monitor it for changes that may justify a different response is a rational reaction.

In other instances, it is appropriate to exploit risk for its opportunity. In times of crisis or disruption, offsetting opportunities can present themselves in the face of emerging risks. In these instances, risk opportunities can serve as a hedge against simultaneous negative risk outcomes. When internal auditors set a good example, clients and other

because of the uncertainty that exists.

In time, this threat will subside. The world is currently experiencing negative outcomes; however, positive outcomes could emerge, such as a more resilient health-care system to deal with similar threats in the future.

### Risk Doesn't Have to Be Scary

When risk is obscure and lurking in the darkness, it seems more like a rattlesnake waiting to strike against an unsuspecting victim. But when risk is visible, understood, and appreciated for its potential benefit, organizations can exploit it for a beneficial outcome or control it to minimize a negative outcome. With this shift in mindset, risk becomes less of a scary monster and more of a device that uses rational decision-making to optimize risk outcomes. 

**RICK WRIGHT, CIA**, is director, Internal Audit and ERM, at YRC Worldwide in Overland Park, Kan.

# spread the word. **TELL THE WORLD.**

---

## **May is International Internal Audit Awareness Month.**

What happens when you tell 5 people that internal audit is indispensable to effective governance?

If all 200,000 IIA members spread the word,  
1 million people will hear our message.



---

Learn how you  
can tell the world.  
[www.theiia.org/Awareness](http://www.theiia.org/Awareness)  
**#IIAMay**



# Fraud Findings

BY GRANT WAHLSTROM + ANISA CHOWDHURY EDITED BY BRYANT RICHARDS

## THE DOUBLE DIPPER

An employee tip uncovers a multimillion-dollar travel and expense scam.

Robert Shull and Alysa Cayden, the forensic audit team at Midnight Sun Inc. (MSI), sat with Justin Planter, a regional sales manager at the solar power company, as he rolled his eyes and made condescending faces. MSI's procurement department forwarded Planter's travel and expense (T&E) reports to Cathy Francis, the human resources manager, after an employee noted that spending was not consistent with the company's T&E policy. Francis reviewed the reports and was concerned that there was a greater pattern of abuse, so she requested that Shull and Cayden examine his T&E reports.

Sitting next to Planter was his boss, Thomas Cooper, a veteran regional manager with more than 25 years of experience with MSI. During the interview, Planter admitted to purchasing a personal cell phone using his company credit card. In

addition, he frequently used the card for alleged business meetings at establishments that bordered on adult entertainment. Much to his surprise, Planter's employment was subsequently terminated.

After the interview, Shull and Cayden felt something was amiss. Cooper approved all of Planter's T&E reports but was not suspicious of any of his spending. Also, they noticed that Cooper's statements were inconsistent, requiring him to revise them on several occasions.

After his firing, Planter contacted MSI's CEO, James Spicolli, and explained how Cooper allowed his management team members to use their corporate credit cards to dine out, make personal purchases, and charge mileage for business travel despite being reimbursed through another program. Planter also claimed that Cooper attended many of the dinners and instructed him to pay the bill so that he could

approve the expenditure, thus avoiding the scrutiny of Cooper's manager. He also alleged that Cooper coached him before the interview on what to say and promised that there would be no significant disciplinary action.

To review Planter's allegations, Shull and Cayden obtained all T&E reports for Cooper and his management team. Data analytics compared the company policy against spending. One area of focus was cash reimbursements for expenses below \$25, the minimum amount requiring receipts to be submitted.

The results were shocking. Cooper's team members used their corporate credit cards for expenses well outside the T&E policy. Furthermore, Cooper approved every expense report submitted to him. They found numerous abuses of travel expenses:

- » Managers split expenses to stay below the \$25 internal control

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





Wolters Kluwer

When you have to be right

# TeamMate+ Expert Solutions

For auditors who are challenged to improve audit productivity while delivering strategic insights, TeamMate provides expert solutions, delivered with premium professional services, to over 3,000 global customers.

**View a Demo Today at:** [TeamMateSolutions.com/Demo](https://TeamMateSolutions.com/Demo)



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

## LESSONS LEARNED

- » Periodically conduct a T&E audit to ensure employees are in compliance with the T&E policy. Review and update the T&E policy and educate employees as part of annual code of conduct training. Low-cost software can review all T&E reports in real time.
- » Management should review subordinates' T&E assumptions during its annual budgeting period. In MSI's investigation, a management team used the T&E budget as a slush fund for personal spending and out-of-policy entertainment.
- » T&E policies should not allow for the use of money service providers (e.g., PayPal). These providers allow for the purchase of goods and services or the transfer of funds for personal use. They also have limited audit trails, which enhances the risk of fraud.
- » The organization should block merchant category codes on corporate T&E cards for goods and services that would not be appropriate for its business or allowable under its T&E policy.

threshold. In one instance, two managers split unknown expenses at a liquor store.

- » One manager submitted for cash reimbursement for client meetings over lunch or dinner for \$24.99 every other day for more than two years.
- » Multiple holiday parties and team meetings were reimbursed, including a substantial liquor bill at each.
- » Team members expensed mileage reimbursement twice.

Shull and Cayden put together detailed profiles on Cooper and each manager, including their expense reports, supporting invoices, and the section of the T&E policy they violated. Additional evidence gathered during interviews resulted in the termination of Cooper and several other managers. Cooper justified the expenditures by explaining he was under budget for T&E expenses on his annual profit and loss statement.

Shull and Cayden then embarked on a companywide T&E audit. They obtained six months of data from MSI's online T&E reporting program. The program allowed employees to book transportation and lodging, code expenditures by spending category, and submit expense reports for approval. Deviations from policy were flagged for the employee's manager to review before approving the expense report.

Shull and Cayden organized and ranked all spending by employee and spending category. Their team selected T&E reports for detailed testing for the most egregious spending by category based on total spending and frequency of policy


violation. Text analysis on words such as "gift card," "baby shower," and "party" identified miscoded or out-of-policy expenditures. They selected samples, reviewed receipts attached to the expense reports, and documented all policy violations. Finally, the investigation team interviewed the employees who submitted the expense reports. Policy violations included:

- » A lack of review by managers of exceptions identified by the T&E program, which flagged millions of dollars of expenditures that were outside policy.
- » Abuse of cellphone reimbursement.
- » Abuse of meal reimbursement, first-class travel, and hotel lodgings.
- » Cash reimbursement where no invoice was submitted to support the expense.
- » Personal spending at online retailers.
- » Spending and funds transfers through money service providers, such as PayPal and Venmo, which have limited audit trails.
- » Purchases of gift cards.
- » Numerous spending violations in Las Vegas, including front row seats to shows and \$1,000 dinners at four-star restaurants.

Individual violations included:

- » An employee transferred \$7,000 from his corporate credit card to his personal business through a money service provider.
- » Employees shared their credit cards with one another when they reached their card limits.
- » A manager sponsored a "kids" event at a local bar.
- » A manager purchased gifts for his secretary at a popular women's lingerie company.

After the investigation, MSI invested in T&E audit software to review all reports in real time. When the software identifies T&E reports with excessive policy violations, the procurement department rejects them. In extreme cases, procurement forwards them to the forensic audit team. In addition, MSI started blocking spending on company credit cards by merchant category codes, which classify businesses by the products or services they provide. The T&E policy was updated to eliminate the use of money service providers.

In most cases of fraud, the employee was terminated. Employees who violated the T&E policy were reprimanded, and demand notices for repayment were sent to employees whose misdeeds were discovered after they left MSI. After one year, T&E spending was reduced by more than \$5 million. 

**GRANT WAHLSTROM, CIA, CPA, CFE**, is the forensic audit manager at a privately held company in Hollywood, Fla.

**ANISA CHOWDHURY, CPA, CA**, is a senior forensic auditor at a security company in South Florida.



# The Responsible Organization

In January, BlackRock CEO Larry Fink published an open letter to company CEOs warning them that if they didn't take immediate steps to help their businesses become more resilient to climate and environmental risks, they risk being dropped from pension fund portfolios. This kind of announcement has the ability to spark boardroom conversations during a time when the push for organizations to identify, mitigate, control, and disclose the myriad risks to their businesses to a wider range of stakeholders—not just shareholders—continues to gather pace worldwide.


Companies now report not only on the financial risks to their business, but also the nonfinancial risks they face. These risks include climate change, business ethics, human rights abuses, slavery and child labor, and their operations' impact on the environment—which fall under the realm of environmental, social, and governance (ESG) reporting. In fact, the current revision of the International Integrated Reporting Council's <IR> Framework aims to “further embed integrated

**Neil Hodge**

**Illustration by Sean Yates**







As investors focus on ESG reporting, there is opportunity for internal auditors to get involved and provide assurance.





reporting and thinking into mainstream business practice.”

Yet despite such reporting progress, the consensus view of several experts is that many organizations are paying lip service, disclosing only the bare minimum of detail to comply or satisfy investors, regulators, and other stakeholders. Some organizations, meanwhile, are struggling to get their heads around what exactly they need to report—or how to do it, they add.

“Sustainability reporting is largely done as a paper exercise,” says Lawrence Heim, managing director at audit and consulting firm Elm Sustainability Partners in Atlanta. He adds that “internal audit needs to be more involved in sustainability reporting, or become involved if it is not already part of the process.” Such views are shared by other experts.

### QUESTIONABLE DISCLOSURES

In the U.K., listed companies have a duty to disclose how sustainability risks may impact the long-term viability of

the business and what steps management is taking to address them. But research from international accounting firm Mazars found that disclosures around carbon emissions in Financial Times Stock Exchange reports are “not fit-for-purpose” and are “in many cases a box-ticking exercise that does not appear to be integral to the way management runs the business.” The Financial Reporting Council, the U.K.’s corporate governance regulator, and the European Union—where sustainability risk reporting has been mandatory for the past two years—have raised concerns about the quality of disclosures around sustainability risks.

Aside from nonfinancial reporting being voluntary for most organizations around the world, there are several reasons why efforts to improve sustainability reporting and risk management are failing. First, the bulk of all mandatory disclosures is still concerned with financial reporting and most of the effort goes into getting that right. Second, the term

*sustainability* has become an umbrella buzzword for every risk that doesn’t have an immediate financial price tag attached to it. Many organizations are either overwhelmed by the scale of work required to report meaningfully on the array of risks included, or are simply confused by the term and the issues being covered under ESG reporting (see “ESG Metrics” on this page).

Experts have some sympathy, but they say that organizations—and internal audit—cannot be indifferent to the problem, and they stress the need for deeper audit involvement.

Heim says organizational sustainability is not clearly understood by either internal auditors or boards, and as a result, levels of assurance are decidedly mixed. Globally, he says there are more than 300 different ratings used by investors to assess ESG reporting, and it is unclear just what criteria they are using to base their assessments.

“There is no agreed on, single definition of what is meant by

## ESG METRICS

The NASDAQ 2019 ESG Reporting Guide 2.0 lists 30 ESG metrics that can provide clarity and direction for internal audit departments getting involved with their organization’s ESG reporting.



### ENVIRONMENTAL (E)

- E1. GHG Emissions
- E2. Emissions Intensity
- E3. Energy Usage
- E4. Energy Intensity
- E5. Energy Mix
- E6. Water Usage
- E7. Environmental Operations
- E8. Climate Oversight/Board
- E9. Climate Oversight/Management
- E10. Climate Risk Mitigation



### SOCIAL (S)

- S1. CEO Pay Ratio
- S2. Gender Pay Ratio
- S3. Employee Turnover
- S4. Gender Diversity
- S5. Temporary Worker Ratio
- S6. Nondiscrimination
- S7. Injury Rate
- S8. Global Health & Safety
- S9. Child & Forced Labor
- S10. Human Rights



### CORPORATE GOVERNANCE (G)

- G1. Board Diversity
- G2. Board Independence
- G3. Incentivized Pay
- G4. Collective Bargaining
- G5. Supplier Code of Conduct
- G6. Ethics & Anti-corruption
- G7. Data Privacy
- G8. ESG Reporting
- G9. Disclosure Practices
- G10. External Assurance

Source: ESG Reporting Guide 2.0. Reprinted with permission from Nasdaq Inc. The complete Reporting Guide is available at [Nasdaq.com/ESG-Guide](https://www.nasdaq.com/ESG-Guide).

# Data availability is the major impediment to developing an explicit process for identifying and assessing climate risks and opportunities, according to the IIF/EBF Global Climate Finance Survey.

organizational sustainability,” Heim says. “The term means different things to different sets of people, and to some extent, it’s an umbrella term for a lot of nonfinancial risks. This is a nightmare for internal auditors.”

## AN EXERCISE IN PR

According to Heim, sustainability reporting is often done cheaply and usually by public relations (PR) or marketing people rather than anyone trained in ESG issues to provide an additional narrative to the financial figures. “These reports are not thorough, not validated, and contain inaccuracies, yet boards are happy to put their names on them,” he says.

There are two trends in sustainability reporting that amount to PR and marketing exercises that Heim says internal auditors need to try to prevent their organizations from following. One is “greenwashing.” This is when companies play up their environmentally friendly efforts and credentials, while downplaying—or ignoring entirely—the areas of their business that may be damaging to the environment, or that do not conform to stakeholder expectations of what constitutes long-term sustainability. The other is “greenwishing,” where they talk about what they hope to achieve versus what they’ve actually implemented. This includes a reduction in carbon emissions, reduced waste, lower energy and water usage, increased telecommuting, cuts in air travel, and so on.

Robert Pojasek, senior strategist at risk and ESG consultancy Strategic Impact Partners in Boston, agrees that sustainability reporting leaves a lot to be desired. “The primary focus of the sustainability report is to improve its ranking in rating schemes, such as the Corporate Knights, Newsweek, Corporate Responsibility Top 100, and similar ratings,” he says. To ensure accuracy and meaningful disclosure, he says, “auditors

need to provide assurance to the board that the information meets their financial, risk, and ESG reporting requirements before it is released to the public.”

## GUIDANCE IS LACKING

Organizations are using stand-alone sustainability programs with separate reporting, which means the claims made in sustainability reports cannot be independently verified or appropriately benchmarked, Pojasek says. As such, there is some reluctance to accept them because of a lack of rigor associated with the collection of the information, as well as a lack of internal auditing of the data-gathering activity. Many investment firms, for example, will not accept ESG information in their sustainability report because it is not complete and it is not independently verified.

Part of the problem, Pojasek says, is that there is little guidance for internal auditors because of the array of functions involved in collecting the data: sustainability teams, consultants, corporate social responsibility teams, and corporate citizenship groups, among others. “It is difficult for internal auditors to understand the sustainability program because there are few practice guides available and auditors are confused by the different kinds of stand-alone sustainability programs,” he says.

Pojasek says internal auditors also may lack knowledge and experience in sustainability reporting because there is no mandatory requirement to do so in disclosures to the U.S. Securities and Exchange Commission, as such information is not often included in Form 10-K and 40-F. As a result, he says, “internal audit knowledge around sustainability programs is probably not as comprehensive as it could or should be as a result of not being involved in this activity.”

Heim adds that voluntary reporting on ESG and sustainability issues often means that while the topics and risks are being discussed, they are not



Internal audit knowledge around sustainability programs is probably not as comprehensive as it could or should be...”

Robert Pojasek





If internal audit approaches sustainability like any other risk assessment, executives will take more notice.”

Douglas Hileman

necessarily being audited. “Internal auditors are not looking at any figures around ESG because they’re not related to financial results, so these figures are published without challenge or any real assurance,” he says.

“It should be impossible for any company report to be made public without checking that the statements are accurate, so sustainability reporting is certainly an area where internal audit can get more deeply involved,” Heim says. “Internal audit has the skills to question the basis of these reports—how they were put together, by whom, and using what information or evidence—and it should have a duty to flag up to the board the risks of publishing material or claims that have not been checked or may be false.”

### A UNITED FRONT

Douglas Hileman, an internal audit, risk, and compliance consultant based in Los Angeles, agrees that internal audit is often excluded from reviewing sustainability strategies and reporting—mainly due to competing priorities and a lack of budget. “There’s very little time, energy, or expertise to look at ESG risks, reputation risk, third-party risk management, human rights, slavery, health and safety, cyber risk, and so on,” he says. “The audit committee decides internal audit’s priorities, and at the moment, sustainability risk is not a top item on their agenda.”

Internal audit can try to address this imbalance. First, Hileman says, internal audit should present sustainability in terms of current and long-term business risks. “Boards and management get risk—a lot of them don’t get sustainability. If internal audit approaches sustainability like any other risk assessment, executives will take more notice.”

Second, Hileman notes, internal audit should present a business case to incorporate sustainability into strategy. Executives need to be talked to in a

language they understand, and they don’t like making investments that don’t pay off. “Provide evidence that shows that acting more sustainably adds value—operationally, in assuring compliance, reputationally, and even financially,” he says. “The area is dynamic, so by acting strategically now they can get ahead of competitors and be better prepared and more resilient for future risks, including environmental risks.”

Third, he says, internal audit should collaborate with other assurance functions—compliance, risk management, environmental, and in-house legal—to “push the case for better aggregated understanding and management of sustainability risk. Clear, concise communication of sustainability risk—and opportunities—can attract the attention and resources it deserves and can also offer a vehicle for internal audit to demonstrate how it can add value to the organization.”

There will be greater scope for internal audit to provide assurance on sustainability issues going forward, says Vanessa Havard-Williams, partner and global head of environment at the London office of international law firm Linklaters. “As organizations—particularly large corporations—begin to integrate sustainability impacts at a detailed level into their enterprise risk management frameworks, internal audit will get more closely involved in reviewing them and providing assurance on their effectiveness to the board,” she says.

“Executives are well aware of the damage that a tarnished reputation can have on the company’s bottom line and customer base,” says Fay Feeney, CEO of emerging risk strategy consultancy Risk for Good and a board member in Hermosa Beach, Calif. “So internal audit should make it clear that an organization’s failure to commit to sustainable business practices will damage the corporate brand among a wide variety of stakeholders, including employees.”

**42%** of institutional investors incorporated ESG factors into their investment decision-making process in 2019, up from 22% in 2013, according to The Callan Institute's 2019 ESG Survey.

Feeney also warns that auditors need to be prepared to acknowledge that board members are overconfident about the organization's capability to manage risks, as noted in The IIA's OnRisk 2020 report. As a result, she says, "internal auditors need to assess their boards' understanding against their knowledge of sustainability risks as there are likely to be gaps in their knowledge and areas where they do not fully understand what needs to be done, and what impact these risks can have on the business, its operations, and supply chains."

### **SPEAK THE SAME LANGUAGE**

Paul Sobel, chair of The Committee of Sponsoring Organizations of the Treadway Commission, says internal audit needs to make sure the board—and everyone else in the business—speaks the same language around sustainability so the issues, risks, opportunities, and the organization's long-term goals are understood in the same way. If everyone involved is thinking about risk in the same way, he says, "it will be easier to discuss and appreciate the risks to the organization—and what responses are needed—in the same way, too."

Sobel adds that internal audit needs to think about the value proposition around sustainability and push the business case for change, rather than follow most boards' leads to consider it as a cost or compliance headache. "Internal audit needs to look at what future investor, regulatory, and stakeholder expectations are likely to be regarding sustainability risk management and reporting and push for management and the board to move in line—or ahead—of them," he says. "This means keeping up to date with best practice, reviewing ongoing trends, and engaging more robustly with stakeholders."

### **CHANGING PRIORITIES**

When 181 U.S. CEOs signed the Business Roundtable's new Statement

on the Purpose of a Corporation last August, they committed to, among other things, "respect the people in our communities and protect the environment by embracing sustainable practices across our businesses." With support from major U.S. companies to adopt sustainable business practices and embed reporting—and practice what they preach—the expectation is that other organizations need to follow suit, if they aren't already.

Internal audit needs to get more involved and leverage sustainability to find potential business opportunities and use them to offset the business threats, Pojasek says. "Auditors need to look for the upsides of risk." To do that, he says auditors need to raise questions that can help their organizations enjoy enhanced value: Are there ways to turn what looks like a costly threat into sustained value for the corporation? Does this provide a better way to make sustainability a key part of how the business is operated to secure long-term financial growth? Does this structured form of sustainability and uncertainty risk afford a new opportunity to look at the supply chain?

There is little doubt of the need for organizations to review their long-term viability and resilience in light of external risks, particularly around the environment and climate change.

If threats such as BlackRock's do not make boards sit up and pay attention—nothing will. And if boards do not make a greater effort to consider sustainability as a key risk issue, it appears likely that shareholders will do so, as evidence shows investors are becoming increasingly activist about how they want companies to be run, and the priorities they want to see in the boardroom. [la](#)

**NEIL HODGE** is a freelance journalist based in Nottingham, U.K.



Internal auditors need to assess their boards' understanding against their knowledge of sustainability risks..."

Fay Feeney



# An RPA

**R**obotic process automation (RPA) has received a lot of attention lately for its ability to streamline processes and increase efficiency. Simply stated, RPA is the automation via virtual robots (bots) of computer-based tasks traditionally performed by people. RPA bots consist of software programs that mimic repetitive actions exactly the way a person would perform them. In the business world, RPA has gained momentum as a tool for automating standard repetitive tasks that require little human judgment or thought. The technology frees up meaningful time for humans to perform work that is, well, more human – tasks that require more analytical or intellectual brain power.

Rudimentary RPA has been around for decades. Spreadsheet macros, for example, have long enabled users to record keystrokes and automate basic tasks with the click of a mouse. Today, RPA bot development is much more sophisticated. Bots are unbound from a single system or database and can manipulate unstructured data – such as by “scraping” it from a screen shot based on a keyword, phrase, or screen location.

The technology’s powerful capabilities have enabled multiple uses of RPA, from automating account reconciliations to performing audit tasks. With these capabilities in mind, the internal audit function at YRC Worldwide (YRCW), a trucking company specializing in freight transportation and logistics services for North American shippers, undertook a pilot program to implement RPA technology. The





# Road Test



Internal auditors at a freight transportation company take robotic process automation for a test drive.

**Rick Wright**



PHOTO COURTESY OF YRC WORLDWIDE;  
ICON: RETRO67 / SHUTTERSTOCK.COM

effort was a success, paving the way for a formal implementation plan and future RPA rollout.

### THE IMPETUS FOR RPA

With a staff of 17, YRCW's internal audit function is organized into two distinct groups—one specializing in regulatory compliance and risk-based, back-office assurance and consulting engagements; the other focused on compliance and operational reviews related to YRCW's network of more than 300 freight terminals. Internal audit's RPA pilot focused on this latter area.

YRCW management has consistently made one request of the internal audit team: Provide more audit coverage with the same amount of staff. In keeping with this challenge, audit leadership strives to innovate and has embarked on a strategic mission to

repertoire of services. Audit leadership saw RPA's potential in this regard as a critical piece of internal audit's strategy. Automating portions of the standard terminal audit program could free up valuable staff resources, allowing more focus on other value-added services.

### PREPARING FOR AUTOMATION

In preparation for the audit of the future initiative and its RPA component, YRCW internal audit leadership assessed several factors. First, leadership examined staff capabilities, with an emphasis on analytical and technology skills. Although commercial RPA tools have become increasingly user-friendly, application development skills can enhance RPA capabilities significantly. And while YRCW internal auditors had upgraded their technology skills over time through individual development plans, they did not possess the desired coding or business analyst acumen to facilitate RPA.

To incorporate these skills, internal audit leadership repurposed one of its analyst roles, which was vacant at the time, and rewrote the job description to include RPA competencies. Requirements included proficiency with SQL or other relevant coding skills. Audit leadership also sought process improvement and business analyst experience—in addition to a background in internal auditing. And while the candidate who eventually filled the role did not possess RPA experience per se, the individual's background and skills allowed for a short learning curve.

Before launching the initiative, internal audit leadership also needed to establish roles for existing team members. They assigned a project lead to learn RPA basics and inform other team members about key features, tools, and requirements. This effort led to a white paper deliverable aimed at defining what RPA was best suited for, identifying key resource needs, and



Part of the department's audit-of-the-future strategy involved enhancing internal audit's value proposition.

create the "terminal audit of the future." Terminal audits consist of transactional and observational testing to provide regulatory and operational compliance assurance, using standard audit programs to provide a consistent measuring stick for evaluating freight terminal performance.

The YRCW audit function has a multiyear track record of year-over-year audit coverage increases. With each successive year, however, these increases become more difficult to sustain. The goal of the audit-of-the-future strategy is to not only increase audit coverage, but also to enhance internal audit's value proposition by adding to its

66% of companies will increase RPA software spending by at least 5% over the next 12 months, according to a 2020 international survey by Forrester Research and UiPath.

## BOT-BUILDING SKILLS

Getting started with RPA does not require specialized skills. Most RPA tools include typical graphical user interfaces with point-and-click functionality that helps beginners get started right away. Anyone with an advanced foundation in the use of basic software tools like Microsoft Excel can develop rudimentary bots. Nonetheless, technical skills such as coding can be helpful when pursuing more sophisticated bot development, especially if the anticipated RPA initiative is more complex.

More advanced RPA tools also provide for customized coding using either SQL or other coding languages. Individuals who leverage business analyst and coding skills can add significant value to more complex bot development projects.

determining whether audit leadership's vision for RPA was realistic. The white paper included a basic description of RPA, as well as information about expected benefits, how RPA works, bot setup options, common capabilities and uses, risks, and top RPA vendors and tools. The document was instrumental in level-setting the team's base knowledge and understanding of the technology's capabilities and limitations. This common understanding enabled the team to collaborate more effectively on a business case for the use of RPA and plan for implementation.

### PROOF OF CONCEPT

Armed with the white paper research, internal audit began working on a proof of concept to determine RPA's potential value related to the terminal audit program. The process consisted of determining which terminal audit program steps might be suited for RPA conversion and highlighting potential efficiency gains. The team identified steps that involved transactional system testing and other system-related test work versus observational steps for which automation would not be feasible.

Team members also estimated the current level of effort required to complete audit steps, designating each one as easy, moderate, or hard. Moderate or hard steps were flagged

as potential candidates for RPA. Steps considered more transactional in nature, and those requiring the auditor to log into multiple systems, were prioritized as optimal candidates. The more difficult and time-intensive the audit step, the better RPA candidate it was deemed. The analysis provided a quantifiable picture of potential time savings, which ultimately affirmed that RPA had the potential to substantially increase terminal audit efficiency. The collaborative analysis and discussions from the proof of concept exercise served as a green light to proceed with a project socialization plan and develop a pilot program.

### SOCIALIZING RPA

With the proof of concept well underway, internal audit leadership began to socialize the initiative with key stakeholders. Socialization represented an important step as the time commitment required to fully implement RPA would potentially impact audit coverage in the near term and might require monetary investment down the road.

Key stakeholders in the socialization effort included internal audit's reporting hierarchy (i.e., the audit committee and the chief financial officer) and operations leadership (the primary audit client). Additionally, support from YRCW's IT team was particularly important, as anticipated



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

transformational benefits required direct access to organizational data.

To gain stakeholders' buy-in and support, internal audit needed them to understand both the long-term benefits and the short-term impacts of the RPA initiative. Socialization involved scheduling brief meetings to educate stakeholders on RPA and its merits. Most of them were familiar with RPA from a business process perspective but had not considered the application as

RPA tool selection is often the first barrier internal audit groups face when looking to pilot an RPA initiative. Especially for smaller internal audit functions, where resources tend to be scarce, monetary investment in a tool that may or may not add substantial value can be a tough sell. Fortunately, several vendors offer web-based RPA tools that provide a basic functionality version, enabling users to get started for free. Internal audit chose this approach

Even when factoring in the manual work required, automation yielded considerable time savings.

it related to the terminal audit process. During the meetings, internal audit also presented the proof of concept results and proposed value proposition for RPA adoption. Because the white paper and proof of concept supported a definitive value proposition, socialization proved merely a formality and the RPA initiative received unqualified support to proceed.

### PILOT BOT

The proof of concept's final phase involved developing a pilot bot. Development consisted of several steps:

- » Identifying an appropriate RPA tool.
- » Selecting a terminal audit program step that would serve as an appropriate candidate for RPA.
- » Working with staff auditors to itemize the tasks required to complete the audit step.
- » Developing the RPA bot logic.
- » Testing, troubleshooting, and refining the bot.
- » Demonstrating the bot.

for its pilot. After reviewing and trying several free tools, internal audit selected one that had an established reputation and appeared capable of accommodating the pilot.

The team chose a pilot audit step that involved several manual audit tasks: logging into multiple systems, navigating to various application screens, acquiring specific lists and fields of data so that a sample of test items could be identified, and analyzing the sample data in a spreadsheet to determine the test outcome. Moreover, anticipated bot efficiencies enabled the auditors to replace judgmental sampling with full population testing.

After defining the new testing approach, the audit team initiated bot development. The process involved recording each of the audit tasks, step-by-step, in the RPA tool. In many ways, development resembled macro programming within a spreadsheet application—auditors captured tasks such as mouse clicks, keystrokes, and login credentials, which they automated using the tool.

### PILOT RESULTS

The pilot project yielded valuable insights about bot development, such as process intricacies often taken for granted when people perform testing. For example, the team realized the value of direct access to data versus indirect access via screen capture. Some steps in the bot development process involved accessing mainframe screens and “scraping” the needed data from them. However, certain application screens consist of mere images and not actual data—i.e., renderings for the user interface. People recognize images easily, but RPA tools vary in their ability to process them. The pilot bot could not recognize data captured as imagery, causing problems at this point in the audit step. The bot would either fail or seize up when encountering this task, requiring manual intervention to complete the step. If direct access to the data could be acquired, the bot would be able to continue processing the audit step to completion. At the time of the pilot, direct access to some of the data was not available.

As a result, the pilot bot produced favorable but incomplete results. The audit step chosen for the pilot usually took an auditor one to two hours to complete manually. Up to the point where screen images proved a barrier, the pilot bot completed the step in about one minute, with an additional 20 minutes of manual processing required by an auditor.

Even when factoring in the manual work, automation yielded considerable time savings. If direct access to data could be obtained, the bot could complete the entire audit step even more efficiently—in two minutes or less. This discovery highlighted the critical value of direct data access to bot development for future RPA roll-out. Through some additional support provided by the IT group, internal audit ultimately acquired direct access



Robotic process automation, Internet of Things, and artificial intelligence are the top three technologies for today's digital strategy, according to a 2020 PwC survey of senior executives.

## THINK BEFORE YOU AUTOMATE

Internal auditors should not undertake bot development projects hastily or without sufficient planning and support. Audit functions looking to pursue RPA should consider:

- » A proof of concept (including pilot) should be performed to ensure adequate value exists to justify the RPA initiative.
- » Rudimentary (free) tools and skills can get the initiative started, but more advanced tools and coding skills may be required to complete the journey.
- » Direct access to data adds exponential value.
- » Partnering with IT or other groups using RPA enables internal audit to leverage internal subject matter expertise and reduce development expenditure.
- » Program quality and sustainability requires close attention to RPA governance.

to the necessary data and completed the pilot bot.

Internal audit compared the bot test results with results from manual completion of work to ensure consistent outcomes. It found that pilot results were of higher quality (full population testing vs. a sample) and significantly more efficient (approximately 90 seconds vs. 1–2 hours to complete the audit step).

### THE ROAD AHEAD

Having validated the potential for bots to increase audit efficiency, YRCW internal audit is now poised to initiate a formal RPA implementation plan. The plan will prioritize audit steps for bot development as well as consider RPA's governance implications. It will address many of the considerations necessary in any IT development environment, including development standards, change management, and user testing.

Internal audit leadership will also need to determine the appropriate post-pilot RPA tool to use, and if necessary, build a business case to justify and secure funding. Additionally, leadership will need to evaluate how to redeploy staff once bot efficiencies start to materialize.

### VEHICLE FOR CHANGE

Like many technology tools, RPA is not a one-size-fits-all solution. Its application model and value potential differ for each organization. Ultimately, the value of RPA lies in automating standard activities that are performed frequently. Internal audit functions whose audit plan includes substantial compliance assurance engagements

Ultimately, the value of RPA lies in automating standard activities that are performed frequently.

that are repeated frequently are likely to have a better business case for RPA than those whose plan comprises a greater proportion of operational and consulting projects. For internal audit functions where RPA makes sense, it can be a game changer. [la](#)

**RICK WRIGHT** is director, Internal Audit and ERM, at YRC Worldwide in Overland Park, Kan.

DON'T JUST ACCEPT INNOVATION.

**Embrace it.**



A helping hand in the face of disruption.

**Welcome to Status Go.™**

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

Audit | Tax | **Advisory**



Grant Thornton LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please see [www.gt.com](https://www.gt.com) for further details. © 2019 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Internal audit can incorporate elements of the Balanced Scorecard approach to build its ability to anticipate and meet the organization's needs.

Basil Orsini

# Audit With Acumen

**B**oard and management stakeholders want internal audit to demonstrate greater business acumen. They want auditors to have a broad understanding of the organization, as well as anticipate how to help the organization achieve its objectives. That means auditors need to see beyond their area of expertise and responsibility. They must be agile to act proactively and congruently with the organization's way of doing business. By recognizing these expectations, internal audit can show that the department is an excellent place to develop business acumen.

## **FIT BUSINESS NEEDS**

Organizations expect all senior managers to have the business acumen to lead their areas of responsibility and support broader organizational success. Managers should be able to anticipate and act on ways to add value to the organization and its stakeholders.

Likewise, internal audit needs to identify the best ways for the function to develop business acumen that fits the organization's needs. It can't take a one-size-fits-all approach,





## Internal audit can build business acumen on a strong understanding and implementation of the *Standards*.

though, because business acumen will vary by industry, type of business, and the kind of service a business unit provides. For example, internal audit will require different aspects of business acumen than business lines, such as sales and production, or support services such as finance and security.

Moreover, internal audit's assurance role in relation to other assurance roles within the organization impacts the kind of business acumen it needs. Developing business acumen can enhance internal audit's risk-based

coverage of the organization's main lines of business, as well as the first two lines of defense.

In developing business acumen, internal audit should not be seen as narrowly focused rule-followers who avoid innovation and taking risks. Chief audit executives (CAEs) should ensure the audit staff understands the capabilities of the organization's first two lines of assurance, as well as the business' main products and services.

Their strategy for establishing business acumen should involve human resource activities, such as hiring, promotions, and career planning, as well as professional development activities.

### ENABLED BY THE STANDARDS

Internal audit's use of business acumen must reinforce, and not compromise, auditors' professional competence. The *International Standards for the Professional Practice of Internal Auditing* place great importance on risk-based planning—multiyear, annual, and engagement—to ensure that services are strategic and add value. Having business acumen enables internal audit to proactively plan and adapt all forms of audit activity to anticipate the organization's assurance needs. This capability goes far beyond simply repeating cyclical coverage or responding to senior management requests.

There is no trade-off between demonstrating business acumen and conforming to the *Standards*. On the contrary, internal audit can build business acumen on a sound understanding and innovative implementation of the *Standards* and associated guidance.

CAEs have used a variety of methods and approaches to attune their staff to the business needs of their organizations. The examples in the boxes that begin on page 41 demonstrate how business acumen can work in internal

Business acumen is one of the **top three** skills CAEs focus on when recruiting, but **39%** say it is very difficult to recruit effectively, according to the 2018 North American Pulse of Internal Audit.

## GOVERNANCE

**T**hese examples can improve mutual understanding, enhance business capabilities, and strengthen relationships at the governance level of the organization:

- » Have the CAE actively participate in regular meetings of the audit committee operational governing body.
- » Assign individual audit managers to each of the major lines of business as account managers.
- » Build the internal audit universe on top of the organization's strategic objectives.
- » Conduct organizationwide internal audits in support of key corporate activities such as internal communications.

audit. These examples are based on four perspectives adapted from the Balanced Scorecard strategic planning and management tool: governance, client, internal processes, and innovation and learning. The boxes substitute governance for the Balanced Scorecard's finance measure. CAEs should plan, track, and report to the board and management on initiatives in each of these areas.

## INTERNAL AUDIT'S ACUMEN

CAEs are likely undertaking some or many of these initiatives, as well as some others. To get the attention and mutual understanding needed, annual internal

## CLIENT

**T**hese examples can improve mutual understanding, improve business capabilities, and strengthen relationships with the organization's business units:

- » Base multiyear, annual audit, and engagement plans on the organization's corporate and business risk profiles.
- » Include strategic upside risks of opportunities and strengths in annual internal audit plans to complement the traditional focus on key downside risks of weaknesses and threats.
- » Reinforce the role of other internal assurance functions (second line of defense), such as risk management and financial control, by auditing their processes.
- » Invite business units to link the timing of audit engagements to their business information needs, such as in support of future financial approval submissions for major initiatives or new programs.
- » Provide information on assessment criteria well in advance of an audit engagement when there are known shortcomings, to enable managers to take corrective action before the audit.

# Work Risk. Not Papers.

root cause

real-time data

business insight

efficiently

connected

committee decks

surveys

evidence

emails

PDFs

Automate the small stuff. Centralize all risk and compliance work on one central platform. Win back more time to spend on the valuable parts of your internal audit work.



Find out more at  
[workiva.com/audit](https://workiva.com/audit)

**workiva**



**Knowledge** of the organization and **its risks** and industry-specific knowledge are among the business acumen attributes spelled out in The IIA's Global Internal Audit Competency Framework.

## INTERNAL PROCESSES

**T**hese internal audit processes can improve mutual understanding and business capabilities, as well as strengthen client relationships throughout the organization:

- » Report more deeply on audit findings by avoiding a narrow-minded approach to audit issues. For example, reports should discuss the broader implications and possibilities of findings, such as their impact on broader business objectives. Internal audit also should show how findings link to implications for other business purposes and recommend reducing inefficient internal controls.
- » Submit periodic status reports on the internal audit plan's implementation and adjust them during the year to better address emerging business assurance needs.
- » Issue periodic reports on significant operational risks based on analyses of internal audit findings within the organization or across the industry.
- » Offer to provide consulting and research services in conjunction with individual engagements.
- » Invite internal audit team members to meet the audit committee and observe its discussion of their individual engagements.

audit plans and year-end reports should include a formal strategy on investments in building staff capabilities to better respond to the emerging needs of the organization. This approach can foster productive discussions and improved understandings with management and the audit committee. [la](#)

**BASIL ORSINI, CIA, CGAP, CRMA, CFE,**  
*is a recently retired internal auditor from the Government of Canada in Ottawa.*

## INNOVATION AND LEARNING

**T**hese examples of innovation and learning can improve mutual understanding, enhance business capabilities, and strengthen relationships:

- » Assign talented employees from other business units to short-term engagements within internal audit. This practice can develop those employees, as well as bring their insight to audit staff members.
- » Send talented internal auditors on developmental, nonaudit assignments within business units. This practice can help those auditors build business acumen and pass their knowledge to the teams with whom they work.
- » Bring internal auditors from field offices to work at headquarters.
- » Train new managers on internal audit's role and areas of expertise such as management control and risk management.
- » Participate in professional associations other than internal audit, such as risk management, IT, security, and fraud prevention. Such groups can help auditors keep abreast of leading practices and share lessons learned with audit colleagues.



Internal audits must delve into the risks posed by the organization's ever-expanding chain of third, fourth, and fifth parties.

**Brian Kostek**

# The Value in the Business Ecosystem

W

hether they know it or not, consumers in today's economy are likely being impacted by an organization's third parties daily. From online merchants, and the delivery partners they use to complete the transaction, to call centers and other support services, third parties support organizations in almost every imaginable way.

In the end, these end-to-end business "ecosystems" are what drive value creation and revenue for today's organizations. Some examples may not be in the control of the organization or its third parties, such as the recent coronavirus outbreak that has had a global impact on operational value chains. And as things go wrong, it is likely that the organization with the brand name is the one impacted and not the third party supporting the product or service in the marketplace.

Understanding an organization's end-to-end processes and how those processes deliver value should be the objective and outcome of an internal audit. That means internal auditors must look beyond third parties to incorporate key fourth, fifth, and sixth parties into planning, scoping, and executing every audit—a process known as "ecosystem management."

## SHIFTING THE EMPHASIS

Focusing on an organization's ecosystem can change the underlying approach and output of an internal audit. Aiming scoping questions, walk-throughs, and outputs at the organization's external partners shifts the emphasis from control gaps, issues,





## Organizations should determine who the third parties of the third party are.

and items requiring resolution to how the business protects its value-driving activities and profit-making ability. This doesn't mean that an organization should change how it plans its annual internal audit schedule. Instead, it should integrate three key principles into how it executes each audit. In other words, the annual audit schedule should continue to focus on higher risk areas, but the scope of each audit should include the ecosystem principles. This approach may result in longer and more complex audits.

### Focus on End-to-end Processes

Audits should focus on the auditable entity and how each process supports the desired inputs and outputs. The scope of the audit of each end-to-end process should include a view of third, fourth, and fifth parties that drive business value. This approach requires auditors to conduct activities as if the external parties are internal to the organization. The audit should demonstrate how the auditable entity delivers value:

through internal people, processes, and technologies only; external parties; or a mix of both.

### Focus on Return on Investment (ROI) and Value-generating Activities

Audits should focus on how each process and end-to-end activity supports ROI generation. If the process doesn't support the organization's ROI, auditors should question its role in the broader organizational ecosystem. The role of external parties in supporting value-generating activities should be a key focus of this exercise.

### Include Business Resilience in the Context of Business Activities

To get operational resilience right requires a change in perspective by management, boards, IT functions, and control functions. For a long time, organizations have focused on determining the probability of an adverse event occurring and ways to prevent it or minimize the damage. As part of this approach, most organizations have developed business continuity and disaster recovery plans, including simulated testing. Business resilience is broader than those traditional topics, though, encompassing business, cyber, infrastructure, and third-party resilience. Internal audit can help drive the broader perspective of operational resilience by integrating these concepts into its ecosystem management approach.

### INTEGRATE PROCESS DOCUMENTATION

When conducting integrated ecosystem audits, internal audit should combine internal and external process documentation into a single and consistent documentation standard. Auditors should communicate this standard to the auditable entity to allow enough time to capture external party documentation in the preferred format, including process and control information.

This approach gives internal audit and other internal parties a single viewpoint on how business activities are driving value and profits. Additionally, it enables internal audit to effectively challenge each auditable entity on the risks and underlying strength of its controls, and how they protect the interests of the organization.

### MANAGE THIRD AND FOURTH PARTIES

Does the organization know who its third parties are and how they support value-generating activities (see "Ecosystem and Extended-party Risk

66% of respondents rate **third-party** relationships as a high **future risk**, an increase from 60% who consider it a high current risk, according to The IIA's OnRisk 2020 report.

## ECOSYSTEM AND EXTENDED-PARTY RISK QUESTIONS

The following examples are questions specific to third-party management that can be used in ecosystem audits:

1. Does a third party support the business activity in meeting its market and customer needs?
2. How does the organization monitor the quality of its third parties and their ability to continue to meet the organization's needs?
3. Does the decision to leverage a third party align with the organization's strategic decisions and key competencies?
4. Does the use of a third party expose the organization to additional reputation and brand risks that must be monitored and managed?
5. What outputs of the process drive value- and profit-generating activities for the organization?
6. Does the use of a third party create potential disruption risks, including impacting the organization's ability to continue to operate and generate value?
7. Does the third party maintain plans to ensure its services would continue in the event of a disruption?

Questions" on this page)? If it does not know, that could spell problems for the organization as a whole and for auditors conducting an audit, as it should be the starting point to completely understanding the ecosystem.

Maintaining a list of contracts and data that does not explain which processes are supported by third parties does little to enhance this understanding. Organizations should go beyond such lists by determining who the third parties of the third party (fourth parties) are. This exercise boils down to two questions:

- » Does the organization understand how it delivers its value proposition to the marketplace?
- » Does that understanding include how its suppliers, service providers, or other entities contribute to that overall mission?

The organization does not need to know every single party within the chain of external relationships. However, it should have a solid understanding of those parties that help to support

its value-generating activities. Parties that have direct inputs are defined as *value-generating*.

Once an organization has an end-to-end view of internal and external processes, it should consider controls among the entities. This requires internal audit to document the operating controls of both the auditable entity and the external parties supporting the delivery of the activity. They also must capture the controls monitoring the transition of processes (hand-offs) between the entities.

That last category becomes more important for key activities that are outsourced to fourth, fifth, or sixth parties. In such scenarios, the organization may rely on an external entity to monitor the quality of delivery of those activities. While this may seem like a lot of additional work, in theory, the business already should have a view of these key activities and monitoring protocols in place to protect its own interests.

If a third party refuses to provide the requested support or documentation,

auditors should still be able to understand how the auditable entity monitors third parties' performance in delivering inputs or services. That knowledge can improve their understanding of the value external parties deliver to the entity.

### LINK TO OPERATIONAL RESILIENCE

Business resilience requires organizations to focus on activities that are critical to their customers and markets, and the infrastructure needed to continue to provide those services. Within ecosystem audits, internal audit should help capture and challenge the business understanding of the end-to-end ecosystem, and whether business leaders are considering all the risks associated with it. Auditors should leverage recent industry and world events as examples to challenge the business on whether it is truly resilient to known and unknown risks to value-generating activities.

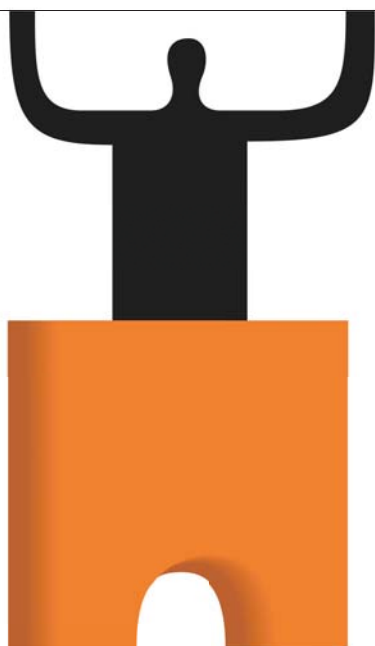
**Identify Critical Services** The organization should identify which of its activities are critical to customers, other market participants, the ongoing continuity of the organization, or the economy. It should prioritize these services for resiliency and have clear tolerances for disruption to those services.

**Understand Impact Tolerance** The organization should use scenarios to estimate the extent of disruption to a business service that it could tolerate. Scenarios should be severe but plausible and assume that a failure of a system or process has occurred. The organization must then decide the point at which disruption becomes no longer tolerable. While using cyber events for such scenarios can focus attention, the organization also should use other events in scenario analysis such as failure of change or IT implementation, and disruption at third parties, outsourced providers, or offshore centers. Senior

management and the board should use the information to update policies and contractual agreements, and drive investment decisions around improving business processes.

**Understand Change Processes** The operational resilience program should evolve with the business as it changes.

### Internal audit should understand the future state of key third parties.



The organization should understand what external or internal factors could change over time and the trends that could impact key business services, and adjust its resilience plans accordingly.

#### FOCUS ON VALUE

Embedded in the audit methodology should be a focus on the business' value-identification, value-generation, and value-realization activities. Every business audit should capture documentation consistently to support the understanding of internal and external processes and controls.

Internal auditors should ask about external entities and collect data to understand the future state of key third parties. They should discuss the criticality of activities and their relation to value-generating activities. Auditors should link the concept of key activities, third parties (and additional parties), and process inputs and outputs to value generation and ROI across the organization. Finally, they should provide an opinion on whether activities are generating the most value possible and whether the business is allocating the necessary resources to meet that objective.

**Business-as-usual Audits** Integrating these concepts into business-as-usual

audits can benefit the organization by focusing on the criticality of value-generating activities. As a result, they can help the organization identify key business risks. During these audits, business personnel typically are more comfortable discussing why the business operates in the manner it does. Moreover, integrated audits limit the need to perform targeted audits on third-party risk, business continuity, cyber risk, and operational resilience.

**Standalone Audits** For organizations that can't integrate these ecosystem concepts into business-as-usual audits, an ecosystem management audit can help them understand how the business delivers value. That understanding is fundamental to gaining a holistic view of the organization's risks. Conducting this audit starts with answering questions about the value delivered to external and internal stakeholders.

Questions for external stakeholders include:

- » What products and services does the organization offer?
- » How does the organization deliver its products and services?
- » What would happen if the organization couldn't deliver its products and services?
- » How does the organization confirm that its products and services are meeting the needs of the market?
- » How does the organization confirm that its products and services are meeting its legal and regulatory obligations?

For internal stakeholders, auditors should ask:

- » How does the organization continue to operate profitably and promote its core values?
- » How does the organization continue to meet board members' expectations?



Outsourcing and **third-party** risk is rated the **No. 4** operational **risk** by risk executives and senior practitioners—up from No. 6 in 2019—in Risk.net’s Top 10 Operational Risks for 2020.

- » How does the organization promote the continued success of its employees and their future well-being?

**Risk Management Program** The answers to these questions can help the organization build core data to support an ecosystem risk management program. The organization can leverage this data across its enterprise risk management frameworks to provide a common taxonomy for how the business drives value.

Moreover, the answers can help the organization address additional questions that could provide a basis for developing an ecosystem mindset for future-state audits:

- » What products and services do we offer, and how do we deliver


them? For example, does the organization provide 100% of products and services through internal processes, or does it rely on third parties to provide 50% of inputs, outputs, or continued servicing?

- » What are the core business objectives, and how does the organization manage them?
- » Does the organization’s culture align with its products and services, and is it consistent with the core business objectives?

#### **A DEEPER UNDERSTANDING OF THE BUSINESS**

Some internal auditors may find the ecosystem management audit concept far-fetched. These professionals may think such audits are beyond their

organization’s capabilities. While this is a reasonable view, those practitioners should keep in mind that without the value the business generates, their role within the organization would not exist.

Internal audit functions should drive value to an organization wherever possible. Standalone audits of value-chain operations can be beneficial to ensuring they function effectively. However, by embedding ecosystem management concepts into business-as-usual activities, internal auditors can drive a deeper understanding of the organization’s value-generating activities and most profitable businesses. 

---

**BRIAN KOSTEK, CRCM**, is a managing director at Protiviti Inc. in Tampa, Fla.

## **Focus** on Team Development in 2020

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

**Our place or your place. Our pace or your pace.**  
[www.theiia.org/2020TeamDevelopment](http://www.theiia.org/2020TeamDevelopment)



Discover additional benefits of group training by calling +1-407-937-1388 or email [TeamDevelopment@theiia.org](mailto:TeamDevelopment@theiia.org). 

2020.0275



Peter Hughes  
Robert Campbell  
John Lerias

# QUESTIONS *on* Culture

Several audit committee FAQs can help guide practitioners when assessing culture.

**A**mong an organization's key assets, perhaps none is more valuable than the culture that permeates it from top to bottom. In the words of management consultant and author Peter Drucker, "Culture eats strategy for breakfast," meaning that even a great strategic plan will likely fail if the organization's mindset and workforce don't align with it.

The word *culture*, as it applies to organizations, refers to the attitudes and workplace behaviors that drive customer and employee relations, the quality of goods and services, and profitability. Recognition of business culture as a legitimate balance

sheet line item under U.S. generally accepted accounting principles underscores that effective culture is a bottom-line essential, not a fuzzy nice-to-have. In fact, a business' culture may carry a book value—in the form of goodwill—higher than any other asset on the balance sheet.

Culture impacts nearly every aspect of an organization, including morale, productivity, and achievement of goals, making it an essential area for internal audit to examine. An FAQ on culture, assembled from years of questions received from audit committees and stakeholders, can serve as a primer on the topic and help guide internal auditors planning to conduct a cultural assessment.

## 1 How is culture formed?

An organization's expressed desire to create an employee- and customer-centric, sustainable enterprise represents nothing more than a wish unless actively supported by the incentives, policies and procedures, and goals established by management. Some of the factors that shape a culture for good or bad include:

- » Employee workloads.
- » Spans of authority.
- » Management style.
- » Ethics policies.
- » Organizational values.
- » Relevance and frequency of training.
- » Recruitment and retention practices.
- » Criteria for employee advancement.
- » Compensation plans.
- » Personnel policies, including work-hour flexibility and remote-work options.
- » Quality controls over products and services.
- » Return policies and product warranties.

An organization's culture is impossible to conceal because it can be observed almost everywhere. It shows, for example, in the level of respect and teamwork among staff members and in the physical work environment. Culture is quantifiable through productivity metrics and by examining compliance with both the letter and spirit of rules and regulations. Moreover, culture is evident in employee turnover rates, and it is undeniably reflected in the organization's success with retaining repeat customers and garnering their recommendations.

Culture is profoundly important to an organization's well-being and competitive viability. The factors associated with a healthy or an unhealthy culture are the same ingredients that determine the quality of goods and services it produces, which in turn affect its very survival.

## 2 Why assess culture?

Every organization will experience some "sway" or "drift" between its desired state and actual behavior. With that in mind, internal auditors should help gauge whether management and staff are acting on values the organization purports to uphold. And while all the components of a culture may support desired attitudes and behaviors at a point in time, they must be continually assessed for relevance and competitiveness for each generation of employee and customer. What's more, some managers do a better job embracing desired values and instilling them among staff than others.

Periodic assessments can identify rogue or ineffective managers—hopefully before they inflict any long-term damage.

Many governing bodies, C-suite executives, and audit committees recognize culture's impact on these and other key organizational factors, including productivity, product and service quality, and the retention and attraction of customers. No company is successful for long by sheer accident and happenstance. Long-term success is achieved only by design and intent that is translated into the tangibles found in organizational culture.

## 3 What are the vital signs of a healthy culture?

The definition of a healthy culture is the same for both the private and public sectors. Health is measured by the degree an organization can sustainably retain committed and capable employees to provide cost-effective, competitive goods or services that are timely and responsive to customers' needs. A sick culture fails in one or more of these critical areas.

Organizational commitment to the integrity of business processes and true customer-centric services are readily apparent, as they permeate every aspect of the operation—from responsiveness to requested information and the usefulness of procedural manuals to workplace civility and the inclusiveness of staff in decision-making. Nonetheless, the presence of these elements does not necessarily indicate a healthy or well-functioning organization—many other factors must be considered.

As such, auditors have found that below-market compensation, poorly structured workflows, unreasonable spans of authority, unrealistic production goals, shortcuts that compromise product and service quality, and absent management are among signs of a dysfunctional culture. Avoiding these deficiencies requires a deliberate commitment from management—one that reverberates throughout the organization.

## 4 What does an assessment of culture involve?

The typical assessment includes soliciting employees' opinions on the degree the organization lives up to its desired cultural values. This information is usually obtained through surveys and personal interviews, and through an examination of pertinent policies and procedures—including codes of conduct, compensation policies, and promotional criteria.





The finished report typically presents:

- » The areas assessed.
- » Employee demographics.
- » The documents, policies, and procedures examined.
- » Responses to each survey question, along with a summary of written comments consolidated into common categories.
- » A blank copy of the survey questionnaire.

Survey reports also frequently include recommendations to address any shortcomings noted. Most assessments are completed within two months.

## 5 Will the assessors rank the culture's various components?

The typical assessment scales comments provided in an interview or survey. Most often, respondents are asked to rank their opinion along a continuum between "strongly disagree" and "strongly agree," or through a similar rating system.

Questions regarding the status of an organization's or subunit's culture are typically grouped into five or more major categories that address values that the board views as its desired corporate identity or personality. These can include innovation, leadership, vision and purpose, collaboration, customer focus, governance and accountability, organizational functionality, adaptability and flexibility, and employee relations. Results commonly present the number of respondents for each of the rankings on the scale, as well as an overall average for each question and category. Survey instruments that enable the reader to gauge the rankings by level of employee, length of service, and gender can be helpful in addressing training, staffing, and funding needs.

Survey results often show that both the executive level and management believe company policies and practices are more closely aligned with the company's desired values than the employees rank it to be. Such insights are essential to stop the "cultural drift" that typically occurs over time.

## 6 Will management get to preview the questions and provide a response?

Cultural assessments should be a collaborative effort that involves management and staff throughout the engagement. Both perspectives are critical in identifying the questions to be asked of survey participants. To succeed, assessments must receive buy-in from everyone involved, which may involve obtaining their perspectives in a written response attached to the report.

## 7 How can auditors prevent assessments from devolving into a complaint session?

Culture assessments typically are designed to avoid being hijacked by a small minority of disgruntled employees. Internal auditors should survey a large population that includes a representative cross-section of positions, salary ranges, operating units, ages, and experience levels, as well as both new and veteran employees. All respondents should provide demographic information, kept anonymous by the assessors, via a dedicated section in the survey instrument. Obtaining this information helps management better assess the validity of the responses.

**58%** of employees and job seekers say company **culture** is more important than **salary** when it comes to job satisfaction, according to a 2019 global survey by Glassdoor.

## 8 Can fiscal, compliance, control, and performance audits be considered audits of culture?

All audits are increasingly viewed as a cultural assessment, but only within the narrow bandwidth of the audit's scope. Many managers and auditors view reports from these audits as an implicit assessment of attitudes and commitment toward assigned duties in light of the organization's values and mission. When performing reviews, auditors may also survey and interview employees from the audited activity as a means of determining whether prevalent attitudes and behaviors reflect the desired culture.

## 9 Should the hotline or whistleblower program be assessed?

Whether or not an organization supports and protects those who speak up when they see suspected misconduct is a critical reflection of its tone at the top. The support and funding for a hotline program, as well as its placement in the organizational hierarchy, sends a signal to employees about the board and CEO's commitment to ensuring integrity in every aspect of the business. Internal auditors should conduct periodic assessments to gauge employees' perceptions regarding the hotline program's value and effectiveness to ensure it continues to promote and support integrity in the workplace.

## 10 Why are internal auditors well-suited to assess culture?

Internal auditors are typically well-regarded and trusted as impartial and objective. Given their exposure to

areas throughout the organization, auditors can regularly observe how the tone at the top impacts employees and the extent to which it shapes desired behavior. This experience gives auditors multiple and varied reference points for comparing best practices, attitudes, and expectations that mold a culture for good or bad. It also helps them offer cost-effective, practical recommendations.

Additionally, auditors are typically well-trained and experienced in assembling evidence and information that supports sound, defensible conclusions. And they are often granted unrestricted access to all personnel, books, and records, as well as cooperation from all affected parties, which removes the typical organizational turf battles and privacy concerns that can thwart other professionals seeking to conduct this type of assessment.

### GETTING CULTURE RIGHT

Every organization has a culture that affects its daily operations, influencing nearly every decision and impacting virtually all employees. Periodic reviews of the culture have proven to foster employee trust and help keep organizations healthy and strong by alerting management to any drift from desired cultural values. When an organization gets culture right, it can make the difference between just surviving in the marketplace and thriving as an industry leader. [la](#)

---

**PETER HUGHES, PHD, CIA, CPA, CFE,** is the assistant auditor-controller-chief audit executive for Los Angeles County.

**ROBERT CAMPBELL, CIA, CFE,** is the division chief of the Los Angeles County Office of County Investigation.

**JOHN LERIAS, CPA,** is the managing partner of GYP in Ontario, Calif.

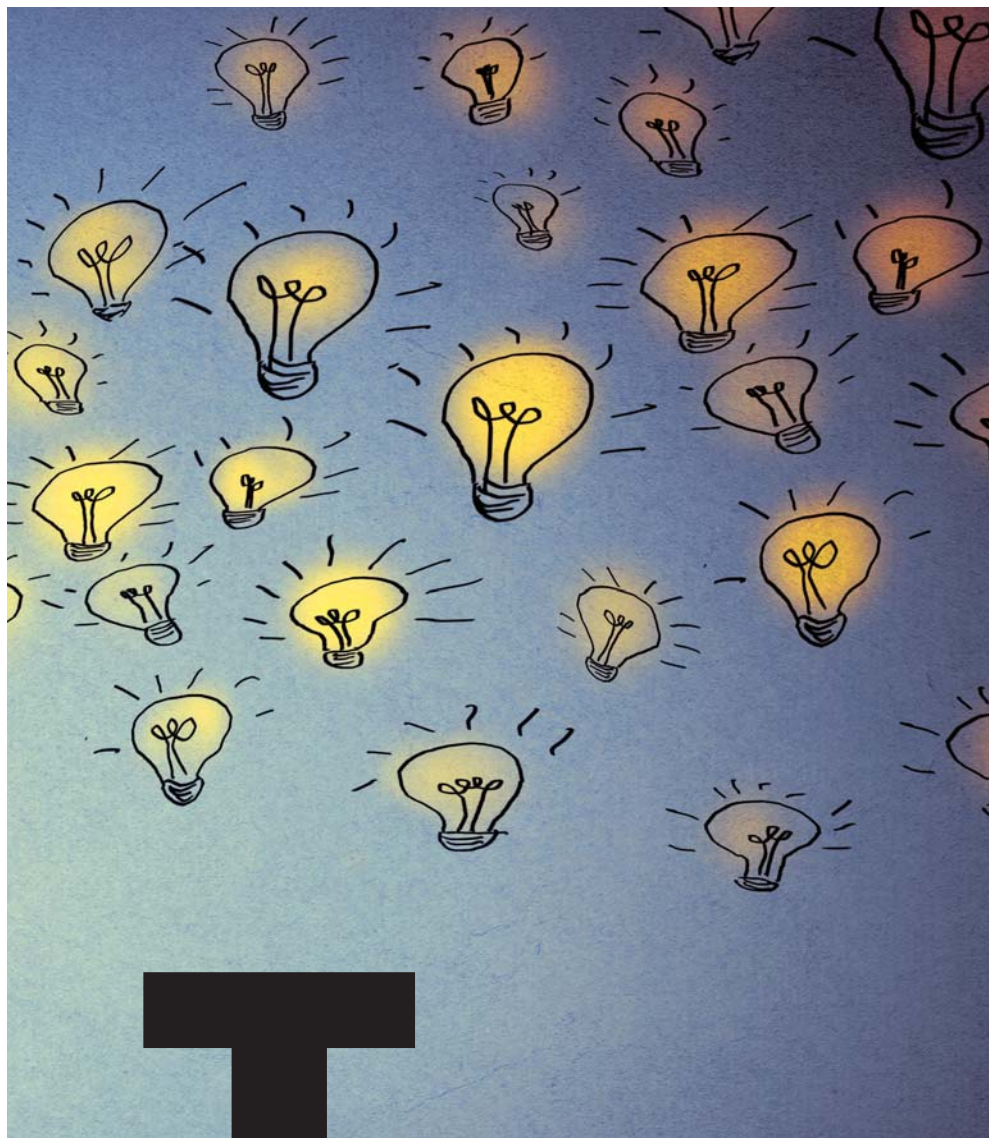
**KEN PUN, CPA,** managing partner for The Pun Group in Newport Beach, Calif., contributed to this article.



# Auditing *Knowledge Management*

Israel Sadu





**Knowledge assets' increased value and contribution to business objectives obliges internal auditors to focus on how they're safeguarded.**

Technological advances are transforming the nature and importance of the organization's knowledge assets—intellectual property, software, data, technological expertise, organizational know-how, and other intellectual resources. The value of the global knowledge management market was around \$2 billion in 2016 and is expected to exceed \$1.2 trillion by 2025, according to Zion Market Research. At this worth, organizations should want to know if their knowledge assets are safeguarded.

Knowledge assets are vulnerable to loss and can be compromised by internal and external sources. In a 2018 study from the Ponemon Institute and Kilpatrick Townsend & Stockton, 82% of respondents acknowledged that their companies very likely failed to detect a breach involving knowledge assets, up from 74% in 2016. Often, audit of knowledge assets is limited to assessing risks, controls, and value derived from the technologies used in their processing (knowledge flow) and



and the digital records maintained that focus on effective document management. This is only a part of knowledge management auditing in the true sense. It does not get to the core issues of the effectiveness of their protection, how they promote business objectives, and the new opportunities they exploit. What has been missing is a structured approach to assess the interplay between strategic and operational risks and controls in enterprisewide knowledge assets management. Unfortunately, there are no comprehensive professional

tends to be a high-risk activity for most organizations. Risks to knowledge assets are any loss that may decrease the potential to effectively pursue an organization's business objectives. Key risk indicators in a typical knowledge-based organization include uncertainties about critical knowledge needs, potential business opportunities lost in their absence, and their impact on business objectives. Other indicators may be process related, such as multiple repositories of information in IT-based systems such as an intranet, collaboration platform, or emails that are not integrated. These indicators can lead to wasted resources and inefficiencies and weaknesses in access restrictions to intellectual property.

Attrition is a common risk involving significant replacement costs that

## Auditors must reorient their methodologies and practices to recognize the role of knowledge assets in achieving business objectives.



guidelines to assess the adequacy of risks confronting knowledge assets, particularly living knowledge assets held by individuals. Internal auditors must adapt to the evolving risk landscape in knowledge management by reorienting their methodologies and practices to recognize the role of knowledge assets in achieving business objectives.

### LOOK FOR RISK INDICATORS

With disruptive technologies at the forefront, knowledge management

can destabilize even the most successful and steady organizations. It is estimated that the average cost of turnover is 1.5 times the annual salary of the job. Internal auditors also should be vigilant about risks specific to tacit knowledge assets management, which include a high tacit-to-explicit knowledge ratio, high staff turnover, a high percentage of core knowledge held by people nearing retirement, and high market demand for key personnel. It is likely in such cases that these assets will be lost.

The passing on of **tacit knowledge** could be **impeded** by the communication skills gap of many Gen Z professionals, according to Deloitte Insights' Generation Z Enters the Workforce.

## EXPLICIT AND TACIT KNOWLEDGE COMPARISON

**T**here are two types of knowledge defined in business. The first, explicit knowledge, is easy to codify, store, and share. It includes textbooks, journals, white papers, patents, literature, audio-visual media, software, and database access. The second, tacit knowledge, comes from personal experience and is not easily replicable or transferable, such as know-how, methodologies, training algorithms, and professional skepticism.

Within tacit knowledge, there are two dimensions: technical and cognitive. The highly subjective and personal insights, intuitions, and inspirations derived from an individual's experience fall under the first category. The second category consists of beliefs, perceptions, values, and emotions ingrained in individuals over years. Some argue that tacit knowledge accounts for about 80% to 90% of the knowledge held in a typical organization. Knowledge assets are created at the intersection of, and interaction between, explicit and tacit knowledge.

## ASSESS STRATEGIC RISKS

Strategy-related risks in knowledge management typically include the absence of, or a weak, knowledge management strategy; lack of involvement from senior management in knowledge management activities; and lack of alignment between key processes and knowledge assets in place.

If knowledge is a key driver for the business or is one of the main products of the business entity audited, such as a consulting firm or an educational institute, internal auditors should ask:

- What is the critical knowledge at risk and who determines it?
- What are the core activities?
- How does information flow through those activities?
- Is there a knowledge management strategy?

Next, internal auditors should remap the business' critical processes to identify what information is needed to run them. If these needs are not being met, they should determine who needs the missing knowledge. Practitioners should review the enterprisewide risk register to assess whether knowledge management-related risks are recognized,

paying attention to the risks of loss of knowledge when core capabilities are outsourced. The instances of high staff turnover and poor knowledge retention among outsourced providers could hamper service quality, involving potential legal risks.

A robust knowledge management strategy should focus on capturing knowledge assets that are critical to success and that underpin performance to create growth and a competitive advantage. Are there sound human resources policies and succession planning strategies for mentor and peer support before, during, and after key staff with the best situational awareness leave the organization? Are there processes to capture results of lessons-learned exercises, particularly with lawyers, consultants, and accountants' knowledge and experience that is incorporated into organizational knowledge and change processes? The knowledge lost in such cases could be costly to replace and may require intensive corrective training or retraining.

In public sector audits, practitioners should pay attention to the procedures followed for valuation of investments in knowledge assets used

to support the provision of public services such as water, transportation, and healthcare. There may not be well-defined standards and methodologies for estimating the social, economic, and financial value derived from the assets as they don't have market-determined equity value.


## ASSESS OPERATIONAL RISKS

Employees spend almost one-fourth of their time searching for information, according to a survey from The Economist Intelligence Unit. Unclear data definitions, ineffective data governance, and poor search engine performance lead to barriers requiring analysts and developers to resolve them. The root cause of most operational risks in managing knowledge assets is lack of alignment between the strategy and the processes built around it.

To start, internal auditors should review the accuracy and reliability of the knowledge assets inventory and the core processes they support, and the responsibilities of the people who manage them. The review results will help identify weaknesses in data governance—such as data silos where data is divided across various databases and divisions accentuating memory loss and poor internal coordination of information. The starting point for the review is identifying and using performance criteria for key activities approved by management. While doing so, internal auditors must be able to determine how the key activities are aligned with key stages of knowledge management in the organization, such as needs identification; acquisition; storage, retrieval, and dissemination; archiving; and performance management. If they do not align, that is a strong indicator that these assets are not generating a tangible return.

Intellectual property in the form of formulae, practices, processes, designs, instruments, patterns, commercial





“My CIA proves I am  
committed to providing  
value to my organization.”

**Emiko Tai, CIA, CCSA**

Japan

*CIA Since 2003*

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



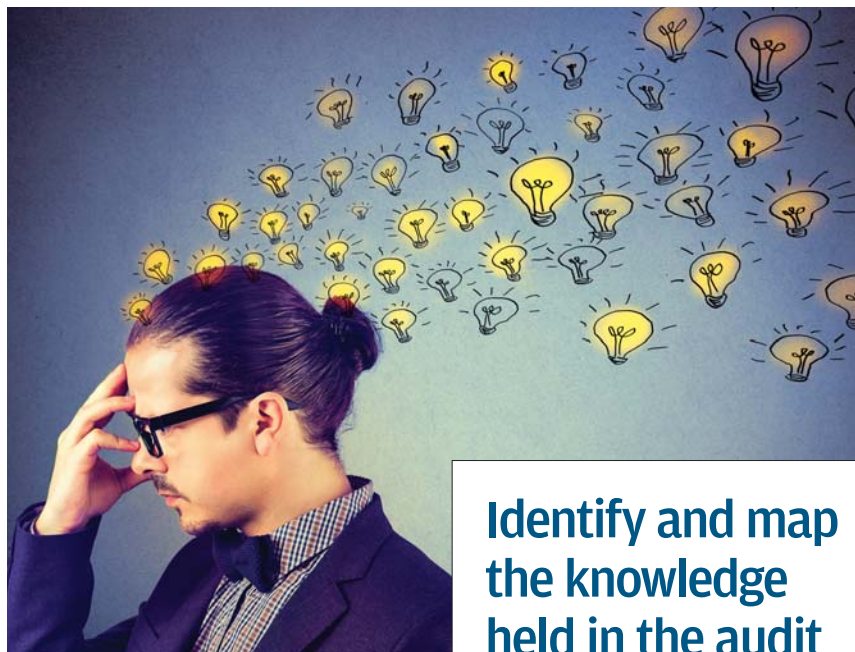
An organization of 1,000 **knowledge** workers wastes **\$5.7 million** annually by searching for but not finding information, estimates International Data Corp.

methods, or compilations of information can be subject to loss or compromised by internal or external sources. Internal auditors should assess that the owners of the intellectual property assets have appropriate controls to prevent cyberattacks that could lead to infringements and inappropriate access.

### INTERNAL AUDIT'S STRATEGY

Auditing knowledge assets requires specific strategies and skills. Each organization's knowledge needs are unique. As internal audit leaders prepare their audit plans beyond 2020, they should have a multipronged strategy to audit their clients' knowledge assets from a value-for-money perspective:

- Retain the best internal audit talent through valuing and investing in the tacit knowledge asset held in the internal audit function.
- Develop and maintain a risk-based audit universe of clients' business operations with significant investments in knowledge assets. This should provide a basis for identifying areas of audit engagement related to knowledge management.
- Identify and map the knowledge held in the audit department to capture and use the tacit knowledge held, particularly related to complex audit engagements. This information could be used to develop an appropriate knowledge management strategy and system to facilitate collaboration within the audit team.
- Empower audit teams to recognize the strategic importance of knowledge assets to the business. This will allow them to provide assurance on legal, commercial, technical, social, and financial aspects of the knowledge assets and the relevant risk indicators. For example, develop a bank of risk indicators—quantitative and qualitative—for assessing the



processes used in tacit knowledge assets management.

- Review the adequacy of audit programs used for knowledge management audits. Strengthen them by focusing on strategic and operational aspects of the processes in place to highlight risks of inefficient use of knowledge assets.
- Focus on the value-for-money aspect of the engagement. Do not get distracted by the technologies and processes used to manage knowledge assets, particularly in engagements involving significant investments in them.

### CLOSING THE GAP

The five most valuable companies in the world report just £172 billion (\$223.2 billion) of tangible assets on their balance sheets, though their total worth is £3.5 trillion (\$454.2 billion). Almost all of their value is in the form of intangible assets, including intellectual property, data, and other knowledge assets, according to a 2018 budget report from Her Majesty's Treasury in the U.K. Despite their critical role in

**Identify and map the knowledge held in the audit department to capture and use the tacit knowledge held, particularly related to complex audit engagements.**

business performance, knowledge assets are not traditionally audited with a focus on how organizations safeguard them to retain their competitive position and how they contribute to business performance. As key partners in the assurance process, internal auditors can take a strategic approach to bridge this gap and maximize its influence. [la](#)

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

# Board Perspectives

BY MATT KELLY

## CAMs AND THE AUDIT REPORT: BRACE FOR IMPACT

Internal audit can help assure a smooth approach for critical audit matters.



BRIAN TREMBLAY



JAN BABIAK



MANU VARGHESE

Internal and external audit teams alike have entered a brave new world in the last year or so, as critical audit matters (CAMs) arrived as items to be included in the external auditor's report. Now comes a crucial question: Will CAMs be an asteroid that slams into the annual audit process—or just a meteor shower that breaks up in the atmosphere?

CAMs are disclosures audit firms make in their audit report, to tell investors what the audit firm deems the most important accounting issues at the company. CAMs involve line items material to the business, and typically their issues will fall into one of two categories. Either the CAM will have weak controls that need attention; or it will be an item that involves subjective, complex judgment no matter how good or bad the controls are.

So far, only large accelerated filers have implemented

CAMs, starting with companies whose fiscal years ended on or after June 30, 2019. All other companies will implement CAMs starting at the end of this year.

One school of thought is that despite all the angst that surrounded the development of CAM requirements in the 2010s, the inclusion of CAMs in the audit report won't do much more than memorialize the same conversations that audit firms and internal audit functions have had for years. But will the process to reach those decisions be substantively different?

"No, not at all," says Brian Tremblay, until recently the head of internal audit at Acacia Communications in suburban Boston. Critical audit matters, he says, are simply where audit firms devote most of their time and attention during the audit. That won't change just because those issues are now written into the audit report.

Tremblay's observation gets at a subtle but important point: what the word "critical" really means here. It does *not* mean that some accounting process is deeply amiss, like a patient in the critical care unit. It only means that the accounting issue is important, in the way that a solid foundation is critical to a whole house.

Now, can that foundation be a rickety mess that threatens the whole structure? Sure. So conversations ensue about how to repair the foundation as necessary. Conversations with audit firms about significant deficiencies or material weaknesses are no different.

"If we were not discussing those things before, we would have been incompetent in our jobs," says Jan Babiak, chair of the audit committee at Walgreens Boots Alliance. She has served on boards where CAMs have come into force both in North America and Europe, and

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





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

says the experience should not catch anyone—audit committee, management, or audit firm—by surprise.

Babiak gave the example of the corporate tax cut enacted by Congress in 2017. Audit committees were discussing the implications of that tax cut with management and auditors before the legislation was even final, let alone enacted. “By the time you get to something being in the opinion, it’s really old news—if you’re competent in what you do.”

OK, so successful implementation of CAMs depends on clear communication with the audit firm about difficult accounting issues. What should that look like for the legions of companies adopting CAMs for the first time this year?

### The Contours of CAMs

One critical step will be a well-defined process to handle significant control deficiencies. A significant deficiency is not automatically a CAM unto itself—although it can be, or it can make a CAM much more likely. So resolving significant deficiencies in a consistent, productive way is crucial.

Manu Varghese, chief audit executive of Hira Industries in Dubai and previously controller at a Big Three U.S. automaker as it adopted CAMs, used a materiality threshold to grade the severity of control deficiencies. Anything that would affect the income statement by less than \$3 million was minor; any effect from \$3 million to \$10 million was major. Any deficiency that had an effect of more than \$10 million was classified as a significant deficiency, or a CAM, “and then management would have to fix it immediately.”

In Varghese’s case, “immediately” was within six months. The internal audit team created an action plan with management, which was presented to the external auditor and then to the audit committee.

What internal audit teams *don’t* want are disputes about significant deficiencies unfolding in front of the audit committee. “If that happens, you’re doing it wrong,” Tremblay says.

Then again, that’s always been the case: Internal audit, management, and the external auditor should have a method to resolve tensions about internal control issues before going in front of the audit committee. So to that extent, CAMs won’t cause any Big Bang change in how financial audits get done.

There’s another type of critical audit matter, too. At least some CAMs will exist simply because they are material to the financial statement and involve, as the audit standard says, “especially challenging, subjective, or complex auditor judgment”—even without any significant control deficiency.

That would be something like assessment of goodwill, contingencies for uncertain tax positions, or reserves for warranties. And sure enough, according to preliminary research

of the first companies disclosing CAMs, the most common subjects were goodwill impairment, tax contingencies, and revenue recognition.

Those CAMs are not necessarily bad; they’re simply important to the financial statements, even if management is rock-solid confident in its judgment about them. “There are things that exist in every auditor’s file regardless of the ‘real’ risk,” Tremblay says. “Those things are just there because they’re judgments and estimates, and that’s the lay of the land.”

Varghese puts an even more philosophical spin on such CAMs. “We need to understand the risk and ask, ‘Can we live with it?’” he says. “If it’s wrong, we fix it. But if it’s just complex—I can live with complex.”


### Whither the Audit Committee

A fair question to ask at this juncture is exactly what the audit committee’s role should be in CAMs. For example, the U.S. Securities and Exchange Commission (SEC) published a statement in December encouraging audit committees “to engage in a substantive dialogue with the auditor” about CAMs and how the external auditor planned to describe them. That’s fine advice, but really the SEC is just advising audit committees to maintain good diplomatic relations with their auditor.

The Public Company Accounting Oversight Board (PCAOB) spent much of 2019 interviewing audit committee chairs, and it found that most chairs already are satisfied with the relationship they have with their audit firms. It’s not like audit committee chairs are straining to dump their audit firms or encouraging investors to deride the audit report at the annual shareholder meeting.

One could argue that all the SEC and PCAOB attention to audit committees is a charm offensive intended to escort board directors past this truth: The audit firm decides what a CAM is—not management, not the audit committee. To a certain extent, audit committees are bystanders here. Sure, they’re bystanders who can protest loudly if CAMs start complicating the message that the board and management want to convey to investors. They are still relatively powerless to stop an audit firm determined to call an issue a CAM.

So the more internal audit and management can work with the audit firm to ensure a smooth, consensus-driven process to handle CAMs, the better. And let’s remember, ultimately CAMs are there to help the investor understand the risks of the company.

“Sometimes people fall asleep reading [audit reports],” Varghese quips. “The CAMs section will probably help focus the attention of the reader, and that’s great.” 

---

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

# YOUR AD HERE

**Put your message in front of your market** with targeted print, online, and digital advertising packages as unique as our 80,000 subscribers in 59 countries.

Contact +1-407-937-1388 or [Sales@theiia.org](mailto:Sales@theiia.org) for details.

***[InternalAuditor.org/Advertise](http://InternalAuditor.org/Advertise)***





BY J. MICHAEL JACKA

## THREE RULES TO AUDIT BY

Practitioners should keep in mind these key recommendations for audit success.

Success as an internal audit professional starts with understanding the basics: risk, controls, planning, testing, interviewing, documentation, reporting, etc. It also requires soft skills such as communication, business acumen, critical thinking, and emotional intelligence. But for the internal auditor who is looking to provide real added value and make a positive impact, those are only table stakes—the bare minimum for getting into the game without being ignored, dismissed, or pigeon-holed as the kind of auditor no one wants to know.

Any internal auditor who wants to be a part of a successful audit future—as well as the future of his or her organization—would do well to follow three rules, listed in reverse order of importance.


**Make Them Care.** We often believe the value of our work is self-evident. That does not mean our clients understand or agree. It is our responsibility to learn what they care about

and align our objectives with those needs. Through that alignment, we need to ensure everyone is working toward the same successes. And an important corollary: If we do not care about our product, organization, or department, then we will fail. How is the client supposed to care when we don't?

**Be a Marketer.** Every internal auditor is in marketing. We are selling the audit, the issues, the report, the need for time with us, the value of our department, and ourselves. Everything we do must include a focus on how we promote our services, the profession, the department, and us, the professional internal auditors.

**Have Fun.** Enjoying the work should be our No. 1 priority. I have seen too many internal auditors—skilled, talented, effective internal auditors—who fail because they have lost their internal audit *joie de vivre* (or perhaps it's *joie de l'audit*). If you are not having fun—if you cannot be excited about what you

are doing—you cannot do your best work. In fact, you probably can't even do good work. Not every minute must be rainbows and unicorns. But every task, project, and opportunity should contain at least a glimmer of possibilities, of excitement—of fun. If we cannot do that, it does not make us bad people, but it probably makes us bad auditors.

And one final note—these recommendations are for every single internal auditor, from those cracking open their first audit program to those who remember working with cuneiform characters on clay tablets. We need to know them when we're first starting out, and we need to be reminded of them every day we work in the profession. We are at our best when we care, when we market, and when we have fun. 

**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)



## CLOUD CONTROL

Cloud computing services are an attractive option, but they come with a multitude of risk and compliance challenges.



**CARRIE FURR**  
Director, Technology  
Risk Consulting  
RSM US LLP



**ERIC LOVELL**  
Practice Director,  
IT Internal Audit  
Solutions  
PwC

### **Why is it important to have an inventory of all cloud solutions in use?**

**FURR** An inventory of all cloud solutions in use within the organization is a critical foundational step in establishing a cloud risk and governance program. The inventory can be a useful tool for understanding the aggregate level of risk to the organization by identifying the data and the number and types of cloud computing technologies being used. The inventory also can be used to manage regular reviews of cloud computing solutions to reduce risk and ensure ongoing compliance.

**LOVELL** Having a complete inventory is the first step in managing the cloud control environment. Armed with this information, organizations can better understand the risks associated with their cloud services; drive clarity regarding roles and responsibilities between vendor and customer; and validate that controls are in place for

security, reliability, agility, and compliance of their clouds.

### **How often should internal audit evaluate solutions?**

**LOVELL** Audit frequency should be based on risk. In a mature organization, internal audit should focus on major cloud projects and migrations, with governance-type audits occurring periodically after the first annual cycle. For an organization just embracing the cloud, internal audit's governance-related reviews should occur more often. For organizations with multiple significant applications in the cloud, I would expect some aspect of cloud is covered every year, via project audits, application audits, integrated audits of functions that use cloud services, infrastructure audits, and those focused on cybersecurity. Importantly, the cloud should be audited where it supports critical business activities that also are under audit.

**FURR** Cloud solutions evolve quickly, and while

organizations typically perform due diligence when choosing a provider, the evaluation often does not address how the platform and individual services develop and are monitored and managed over time. Organizations should perform a cloud computing assessment before completing an audit. Performing an assessment first enables internal audit to build relationships and educate stakeholders on the policies, procedures, and controls necessary to mitigate cloud computing risks. Audit frequency depends on the maturity level, complexity, and use of cloud solutions. As the maturity level of the cloud risk and governance program increases, evaluation frequency can be reduced but should be annual until then.

### **How can internal audit gain assurance around cloud solutions?**

**FURR** The first step is to understand the maturity level of the organization's

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)

## A FOCUS ON CONTROLS

There are several general policies and controls organizations can implement in regard to cloud solutions. At a minimum, RSM's Carrie Furr says, cloud computing requires policies, procedures, and controls around high-risk cloud controls domains, as defined by the Cloud Security Alliance Cloud Controls Matrix:

- » Data security and information life-cycle management.
- » Encryption and key management.
- » Identity and virtualization.
- » Interoperability and portability.
- » Supply chain management, transparency, and accountability.

In addition, PwC's Eric Lovell offers four foundational areas of focus:

**1. Controls related to strategy and governance.** Organizations must determine when and how they move to the cloud, and should develop an architectural reference model to help ensure decisions are consistent

across the enterprise, meet business requirements, provide a return on investment, and are within the company's risk tolerance.

**2. Solution development.** Whether it's an in-house development team using a DevOps approach to deploy and manage applications in cloud infrastructure, or taking advantage of the many enterprise class applications provided as a service, specialists should be involved throughout to make sure adequate controls are in place for the production environment.

**3. Training and awareness.** Both end users and technologists need to be trained on the cloud and how to leverage those services to the advantage of the organization while managing risk.

**4. Controls related to inventory management.** Organizations need an accurate inventory of all cloud services along with sufficient information about each to make informed risk-based decisions. And, organizations need to control the use of unauthorized cloud services.

cloud risk and governance model. Next is understanding the current aggregate cloud computing environment. The final step is understanding the plan to expand cloud-computing solutions. By understanding these three components, internal audit can better identify and help manage and monitor the cloud environment. It should ensure the organization is building its cloud strategy with compliance and risk in mind. The organization should follow a holistic, robust cloud standard.

**LOVELL** First, internal audit should test key controls related to the procurement and deployment of new cloud services. Validate that decisions to move a service into the cloud are based on an established architecture and information security standards to which all parties have committed. Also, validate that standard terms and conditions, as well as service-level agreements, are in line with corporate policy. Second, internal audit should audit the vendor management program. Vendor monitoring should be based on risk and could include review of third-party trust reports, control questionnaires, and on-site visits. Third, internal audit should test controls to identify and limit unauthorized cloud services. Finally, internal audit should get involved in cloud projects and validate controls are in place to ensure the security, compliance, agility, and reliability of the organization's clouds.

### What are some tips for determining whether the audit function is capable of assessing cloud solutions?

**LOVELL** The collective team must understand the technology as well as the business. Look at the current IT audit plan. If the last three years have seen significant coverage of IT infrastructure, cybersecurity, and IT controls that touch application life-cycle management processes, you likely have in-house staff who can learn and cover basic cloud governance, security, and operations-related cloud audits for medium-risk cloud services. However, for any cloud services that support critical business processes or house sensitive data or regulatory compliance-related services or data, supplement audits with subject-matter specialists. Conversely, if the audit plan has historically been focused on IT general controls or application controls, seek outside assistance in general for cloud-related engagements.

**FURR** At my company, we frequently work in partnership with internal audit resources and other key stakeholders to "teach them to fish." Most internal audit teams have little to no cloud computing experience in identifying and managing cloud risk and compliance challenges. This model allows experienced advisors to train their staffs during initial assessments/audits, so they can conduct future cloud computing assessments and audits. [la](#)

# 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)

**la**  
INTERNAL AUDITOR

2017-0409



# IIA Calendar



## IIA CONFERENCES

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

**JULY 20-22**  
**International Conference**  
Miami Beach Convention Center  
Miami

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

**SEPT. 11-13**  
**IIA Canada National Conference**  
TELUS Convention Centre  
Calgary, Alberta

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

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

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

## IIA TRAINING

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

**MAY 12-15**  
**Multiple Courses**  
Minneapolis

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

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

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

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

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

**JUNE 1-12**  
**CIA Exam Preparation – Part 1: Essentials of Internal Auditing**  
Online

**JUNE 2-5**  
**Multiple Courses**  
San Francisco

**JUNE 2-11**  
**Critical Thinking in the Audit Process**  
Online

**JUNE 9-12**  
**Multiple Courses**  
Houston

**JUNE 15-26**  
**CIA Exam Preparation – Part 3: Business Knowledge for Internal Auditing**  
Online

**JUNE 16-19**  
**Multiple Courses**  
Orlando, FL

**JUNE 23-25**  
**IT General Controls**  
Online

**JUNE 23-26**  
**Multiple Courses**  
Philadelphia

**JUNE 23-26**  
**Tools & Techniques I: New Internal Auditor**  
Boise, ID

**JULY 7-10**  
**Multiple Courses**  
Denver

**JULY 7-16**  
**Audit Report Writing**  
Online

**JULY 13-22**  
**Cybersecurity Auditing in an Unsecure World**  
Online

**JULY 14-22**  
**Multiple Courses**  
Lake Mary, FL

**JULY 14-23**  
**Root Cause Analysis for Internal Auditors**  
Online

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





BY AYSHA AL SHAMSI

## DIVIDED BOARD LOYALTIES

Internal audit independence can suffer when board directors' priorities are split in two.

An organization's board of directors is essential to good governance. It can provide an independent, authoritative voice on key decision-making, help guide strategic thinking, and contribute to organizational integrity. But lack of true independence can dampen that support. Board priorities may teeter between what's good for the organization and what executive management or shareholders would prefer, which often may be at odds. Divided board loyalties can be detrimental to organizational governance, and particularly to the internal audit function.

In a worst-case scenario, the board of directors may try to influence internal auditors' activity indirectly or steer policies to best match shareholders' interests, resulting in a loss or weakening of internal audit value and independence. Moreover, because the organization's top management answers to the board, internal audit's independence could be further impaired in situations where the CEO also serves as a board member. It also introduces the

possibility of ethical lapses and other wrongdoing.

Of course, effective oversight—and internal audit—requires a qualified audit committee. In part, the committee should help ensure that internal auditing is not influenced by top management. And according to IIA Standard 1110, internal audit achieves organizational independence effectively “when the chief audit executive reports functionally to the board.” But given its positioning as a sub-unit of the board, and the board's responsibility for appointing audit committee members, the committee may still show allegiance to executive priorities—even when they conflict with effective governance practices. If the board's support of internal auditing is weak, the audit committee's support, in turn, may also fall short.

Boards of directors focused exclusively on shareholder interests, emphasizing share price and profit generation, may believe their only responsibility is to increase the organization's value. In fact, with today's hyper-competitive global market, companies face more and more

pressure to increase profits, potentially at the expense of following regulations or company policies. And if internal audit's reporting might negatively impact those priorities, then the risk of its findings being discarded or ignored are heightened. That risk is further exacerbated with audit committee members also serving on the full board, as they may be more inclined to agree with boards or executives who deprioritize the need for effective governance.

Still, many organizations—particularly in the public sector—do not have audit committees or the equivalent of a board-level presence. Oversight structures that include a board and audit committee, while flawed, at least provide a measure of governance assurance and support for internal audit independence. But auditors need to be aware that the potential for divided board loyalties is a risk in nearly every organization, and the possibility of compromised oversight is a very real one. [16](#)

**AYSHA AL SHAMSI** is an internal auditor at Ajman Tourism Department in the United Arab Emirates.

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

# MEMBERSHIP MEANS MORE INDUSTRY-SPECIFIC CONTENT

*Specialty Audit Centers Now Included With Membership*



**Your IIA membership** now includes full access to our Specialty Audit Center resources at no additional cost. Discover a vast network of industry-specific content you can't find anywhere else, created and aggregated to keep you influential, impactful, and indispensable.



**Learn more.** [www.theiia.org/SpecialtyCenters](http://www.theiia.org/SpecialtyCenters)

Financial Services | Public Sector | Environmental, Health & Safety

# Go Audit. And Beyond.

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

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



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

Top Rated Audit Software On

