

JUNE 2017

INTERNALAUDITOR.ORG

San Diego Schools *Approve Plan to Gut* *Internal Audit* *Department*

INTERNAL AUDITOR

PUBLIC SECTOR AUDITING UNDER SIEGE

Suspended HISD Chief Auditor:
‘This district does not want the
real dirt to be published’

Former Auditor Sues
DPHHS Over Firing
Duggan Aide Accused of
Obstructing Audit Contracting
Everybody Loves a Watchdog ...
Until It Barks



WE DON'T JUST FOLLOW RULES.
WE HAVE STANDARDS

Internal auditors are not just a bunch of rule followers.

We're solution-focused and principle-minded. Standards-driven, framework-followers. As a matter of fact, global industry experts at The IIA develop, document, and deliver the standards of the profession. The *International Standards for the Professional Practice of Internal Auditing* help all internal auditors be more effective.

You won't believe how helpful it is to have standards.

Standards Practice Makes Sense
www.theiia.org/WeHaveStandards

 **The Institute of
Internal Auditors**

Rearview mirror?

Crystal ball?

Ask us how our market-leading global risk and internal audit practices help the internal audit function look beyond assurance to provide business insights and help management anticipate risks.
ey.com/advisory



2017 ENVIRONMENTAL, HEALTH & SAFETY EXCHANGE

Connect. Collaborate. Evolve.

SEPT. 11-12

Hyatt Regency St. Louis / St. Louis, MO

Turning Risk Into Readiness!

In 2015, EPA and OSHA fines cost U.S. organizations over \$13 billion, however, only 11% of CAEs rely on internal audit to provide EHS assurance to the board.

The EHS Exchange is the premier conference dedicated to the development and professional practice of environmental, health and safety (EHS) auditing, providing audit professionals with high-quality, specialized training, and networking opportunities with industry peers.

Who Should Attend?

- EHS, Process Safety Management, and Product Stewardship Auditing Professionals
- Internal auditors who recognize the importance of learning how to identify and manage EHS risks and bringing additional value to an organization
- Those interested in understanding the full breadth of the potential impact of EHS risks

Register today!

www.theiia.org/EHSExchange



**Environmental
Health & Safety**
AUDIT CENTER



FEATURES

24 COVER Under Siege Public sector auditors can face intimidation, isolation, retaliation, suspension – even termination – just for doing their job. **BY RUSSELL A. JACKSON**

30 How to Audit Culture Culture audits can help practitioners gain insight into the causes of poor organizational behavior. **BY JAMES ROTH**

39 A Smarter Approach to Third-party Risk Adopting a focused, collaborative strategy can help improve management of outsourced service providers. **BY MICHAEL ROSE AND DENNIS FRIO**

44 The Innovative Internal Auditor As businesses strive to find opportunities in a world driven by technological transformation, internal auditors need to continually innovate

to stay ahead of the game, says **SHANNON URBAN**, 2017-2018 chairman of The IIA's North American Board.

50 The Dynamics of Interpersonal Behavior To be successful, auditors need to cultivate their soft skills just as much as their technical abilities. **BY ARTHUR PIPER**

57 Opportunity From Disruption Adopting six traits can enable internal audit functions to become more agile in the face of change. **BY JASON PETT, MARK KRISTALL, AND DEBORAH MACK**



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



Trust Your Quality to the Experts

Building confidence with your stakeholders through a solid Quality Assurance and Improvement Program (QAIP) is unique to each internal audit activity. The first challenge may be where to start. IIA Quality Services is here to provide guidance and resources to assist in defining the way.

Look to IIA Quality Services' expert practitioners to provide:

- Insightful external quality assessment services.
- Generally Accepted Government Auditing Standards (GAGAS) reviews.
- On-time solutions and successful practice suggestions based on extensive field experience.
- Enhanced credibility with a future-focused assessment.

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



DEPARTMENTS



7 Editor's Note

8 Reader Forum

67 Calendar

PRACTICES

11 Update Terrorism and political violence increase; new bank security standards released; and leaders set wrong tone.

15 Back to Basics Auditors should regularly perform key stakeholder surveys.

18 ITAudit Application controls represent a risk that should be tested.

20 Risk Watch Gaps in the control environment may introduce unacceptable risk.

22 Fraud Findings Analytics reveal prepaid cards being used to boost commissions.

INSIGHTS

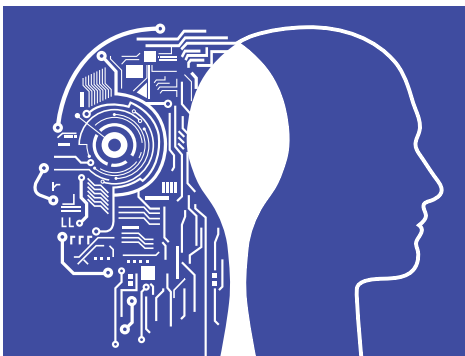
61 Governance Perspectives New privacy regulation is an important part of the organization's governance model.

63 The Mind of Jacka What excuses are keeping you from effecting change?

64 Eye on Business Courage is a prerequisite of the job.

68 In My Opinion Maybe internal auditors should embrace the corporate cop image.

ONLINE InternalAuditor.org



Where AI Meets EQ

The future of internal audit work may well lie at the intersection of cognitive technology and emotional acuity.

Risk Management in the Public Sector Watch a video discussion on the unique challenges of managing risk in government organizations.

Red Card for Fraud

Fraud expert Art Stewart discusses FIFA's recent suspension of an audit committee member who was convicted of bribery.

Auditing Cyber Resiliency

Internal auditors need to provide assurance over eight categories of resiliency.



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

Ia
INTERNAL AUDITOR



COURAGE UNDER FIRE

For every headline about public sector auditors under fire for doing their jobs, there are many others about the good work these auditors do:

- “Internal Audit Finds Risk in Chatham County Public Works’ Payroll Records”
- “Audit Finds Fraud, Illegal Spending at Southern Ohio Correctional Facility”
- “Audit Finds \$30 Million in Bookkeeping Errors in Sarasota Pensions”
- “Audit: 25% of City Workers Tested Had Errors in Expense Reports”
- “California Audit Clears L.A.’s Largest Charter School Network of Misspending”

Internal Auditor’s Twitter newsfeed @IaMag_IIA regularly posts articles about the latest findings by public sector auditors. Unfortunately, the feed also frequently includes posts about public sector auditors being treated badly.

According to The IIA’s Global Public Sector Insights report: *The Role of Auditing in Public Sector Governance*, auditing is a cornerstone of good public sector governance. “By providing unbiased, objective assessments of whether public resources are managed responsibly and effectively to achieve intended results, auditors help public sector organizations achieve accountability and integrity, improve operations, and instill confidence among citizens and stakeholders,” the guidance says.

So why are so many public sector audit functions under siege? Often it’s due to the political agendas so prevalent in the public sector. Auditors who bring issues to light often face retribution, even termination.

In this month’s cover story (page 24), several public sector auditors share their horror stories, some anonymously, in the hopes of helping auditors in similar situations. Although it may sometimes seem like there’s no solution, there are actions auditors can take to ward off these issues. According to author Russell Jackson, in many cases “targeted relationship-building and a firm grasp of the agency’s governance structure will go a long way toward avoiding catastrophe.”

It takes courage to be a public sector auditor today; in fact, courage is a prerequisite of being an internal auditor, in general. Auditors in all sectors can feel pressure and face retribution just for doing their jobs. In “Speaking Out” on page 64, Greg Grocholski, chief audit executive at SABIC, and Dan Williams, senior vice president, Internal Audit, at Darden Restaurants, discuss the challenges of reporting fraud or misconduct at the executive level in the corporate world.

As Grocholski states, “If you are trusted, if you are professional, if you are seen as objective—and not pursuing an agenda—I firmly believe, based on my own experience, that you will have that support when needed.” Those are welcome words to a profession that is constantly challenged to go where others may fear to tread.

@AMillage on Twitter

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



organizations have to decide: Do I pull valuable first-line resources to perform self-assessments and testing, or do I devote dedicated resources (not internal audit) with expertise in performing these tasks?

JACK AMODEO comments on Susan Burch's "Three Lines in Harmony" (April 2017).

I was impressed with "Three Lines in Harmony." The word *defense* evokes a reactive image, but the original concept is rather proactive for the benefit of the organization. I work for a financial institution. To be trusted by customers, it's imperative to be/become a sound and prudent company. Especially while in the throes of a financial crisis, tightening regulatory compliance and performing many routine self-checks proved beneficial. But, after blindly following it for a decade, we're trapped and boxed in the stagnation of compliance fatigue. To increase harmony across the three lines of defense, as an internal auditor, I'm willing to establish communication with members of the first and second lines and to take

a proactive role in implementing the centralized testing model.

HARUKI KUMOI comments on Susan Burch's "Three Lines in Harmony" (April 2017).

Shift of Focus

Great insight from Bruce McCuaig. I think this requires a paradigm shift and heads of internal audit need to drive this change. I come from an IT audit background and over the course of my career I have realized that auditors need to evolve and spend more time on evaluating business risks and providing input to risk management rather than conventionally evaluating the control effectiveness.

RAHIM ALI comments on Bruce McCuaig's "Time for Internal Auditors to Get Out of Control" (Internal Auditor.org, April 2017).

You Cannot Dictate Culture

I think the issue is often that senior leadership is so insulated from the pulse of the organization that they only are able to gauge the real culture of their mainline employee base through the input of their direct reports or through surveys, which Norman Marks rightly notes will not

ROI of Resources

I found Susan Burch's article interesting regarding the centralized testing model. Whether an organization is public (preserving and safeguarding its resources to protect the public's best interest) or private (focusing on owners' risks), the time and resources it devotes to performing risk assessments and testing controls has to be optimized to provide the best return on the investment of these resources. It is generally advantageous to keep "first-line subject matter experts" focused on core mission objectives. So

Ia
INTERNAL
AUDITOR

JUNE 2017
VOLUME LXXIV:III

EDITOR IN CHIEF

Anne Millage

MANAGING EDITOR

David Salierno

ASSOCIATE MANAGING EDITOR

Tim McCollum

SENIOR EDITOR

Shannon Steffee

ART DIRECTION

Yacinski Design, LLC

PRODUCTION MANAGER

Gretchen Gorfine

CONTRIBUTING EDITORS

Mark Brinkley, CIA, CFSa, CRMA
J. Michael Jacka, CIA, CPCLU, CFE, CPA
Steve Mar, CFSa, CISA
Bryant Richards, CIA, CRMA
James Roth, PhD, CIA, CCSA, CRMA
Laura Soileau, CIA, CRMA
Charlie Wright, CIA, CPA, CISA

EDITORIAL ADVISORY BOARD

Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, CGA, FCIS, CFMA
Mark Brinkley, CIA, CFSa, CRMA
Robin Altia Brown
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Wade Cassels, CIA, CCSA, CRMA, CFE
Daniel J. Clemens, CIA
David Coderre, CPM
Michael Cox, FIA(INZ), AT
Dominic Daher, JD, LL.M.
Haley Deniston, CPA
Kayla Flanders, CIA, CRMA
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA

Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
Karin L. Hill, CIA, CGAP, CRMA
J. Michael Jacka, CIA, CPCLU, CFE, CPA
Gary Jordan, CIA, CRMA
Sandra Kasahara, CIA, CPA
Michael Levy, CIA, CRMA, CISA, CISSP
Merek Lipson, CIA
Thomas Luccock, CIA, CPA
Michael Marinaccio, CIA
Norman Marks, CPA, CRMA
Alyssa G. Martin, CPA
Dennis McGuffie, CPA
Stephen Minder, CIA
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Bryant Richards, CIA, FCIS, FIA
Jeffrey Ridley, CIA, FCIS, FIA
Marshall Romney, PhD, CPA, CFE
James Roth, PhD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debra Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PhD, CPA
Glenn Summers, PhD, CIA, CPA, CRMA
Sonia Thomas, CRMA

Stephen Tiley, CIA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoor, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CFSa, CRMA
Benito Ybarra, CIA

IIA PRESIDENT AND CEO

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

IIA CHAIRMAN OF THE BOARD

Angela Witzany, CIA, QIAL, CRMA



PUBLISHED BY THE
INSTITUTE OF INTERNAL
AUDITORS INC.

CONTACT INFORMATION

ADVERTISING

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

SUBSCRIPTIONS, CHANGE OF ADDRESS, MISSING ISSUES

customerrelations@theiaa.org
+1-407-937-1111; fax +1-407-937-1101

EDITORIAL

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

PERMISSIONS AND REPRINTS

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

WRITER'S GUIDELINES

[Internal Auditor.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.

capture an honest picture of the organization. Leaders must get out among the employees, have conversations, and build trust directly—not through intermediaries—to see, feel, and experience the culture of the company. Culture cannot be dictated, it must be demonstrated and shared to generate the sort of buy-in by the employee base to assure ongoing adoption and adherence.

PAUL B. *comments on the Marks on Governance blog post, "Culture May Be the Wrong Question."*

Keeping Control

When outsourced, it's key that senior management and the board keep in

mind that they should always be able to understand in depth the outcomes of the internal audit function. Otherwise, control is out of your hands.

PAUL VAN DER ZWAN *comments on the Chambers on the Profession blog post, "Outsourcing Internal Auditing: Dos and Don'ts."*

A Lack of Risk Awareness

It is difficult to Monday morning quarterback on this topic without knowing for sure whether United's enterprise risk management (ERM) process was used during the development of the referenced policy. However, it becomes clear that there was no risk awareness built

into the company's decision-making process. Regardless of being management or front-line staff, employees should have a framework or questions, such as the ones Marks proposed, that should be an automatic response to this type of situation. But in reality, this situation wouldn't have happened if management had truly involved—and listened to—its ERM program.

CAROL WILLIAMS *comments on the Marks on Governance blog post, "Risk and the United Airlines Fiasco."*



VISIT InternalAuditor.org for the latest blogs.

A COLLAPSE IN IT SECURITY ISN'T JUST A LEAK...

IT'S A FLOOD

SECURANCE CONSULTING

IT RISK ASSESSMENT • IT SECURITY • COMPLIANCE • PEACE OF MIND

SECURANCECONSULTING.COM 877.578.0215

2017 GRC

Where Governance and Risk Management Align for Impact

Keynote John Sileo to Share His Story of Dramatic Transformation



Hear firsthand the extraordinary experiences of John Sileo, keynote speaker at the **2017 Governance, Risk, and Control (GRC) Conference**, Aug. 16–18, in Dallas-Ft. Worth, Texas, USA. Sileo is an award-winning author and cybersecurity expert who has appeared on *60 Minutes*, *Anderson Cooper*, and *Rachael Ray*. He also spent two years working to stay out of jail.

Learn why he was in this predicament, as Sileo focuses on managing privacy and reputation in an economy plagued by digital overexposure.

EARN UP TO
18 CPE HOURS.

SAVE US\$200
WHEN YOU REGISTER
BY JUNE 12, 2017!

Register Soon—space is limited and previous events have sold out!

www.theiia.org/GRC



Securing global banking systems... Corrupt practices remain widespread...
Management tone crucial to culture... Devices raise e-discovery risk.

Update



THE HIGH RISK OF INACTION

Only a small percentage of U.K. businesses exercise good security practices to combat cyber threats.

37%

Segregated wireless networks

33%

Formal cyber risk policy

32%

Document cyber risks in business continuity plans, internal audits, or risk registers

29%

Board members responsible for cybersecurity

Source: U.K. government, Ipsos MORI Social Research, and University of Portsmouth, Cyber Security Breaches Survey 2017

TERRORISM AND GEOPOLITICAL RISK

Violence and political uncertainty threaten business interests internationally.

A 14 percent rise in terrorist incidents globally in 2016 and a wave of populism are contributing to increasingly volatile operating conditions for international business, according to risk management, insurance, and reinsurance provider Aon plc.

The firm's 2017 Risk Maps report, produced in conjunction with Roubini Global Economics and The Risk Advisory Group, also found that while terrorist strikes increased by 174 percent in the U.S. and Europe, attacks on those countries account for less than 3 percent of terrorist violence globally. Last year, the number of

terrorist incidents in the U.S. was the highest it's been in a decade, though the Risk Maps report notes that the threat will likely be moderate in 2017.

More country risk ratings in 2016 increased (19) than decreased (11), marking the second year in a row this has occurred. Moreover, the report notes that overall terrorism and political violence ratings are at their highest levels in four years. A total of 17 countries are currently at highest risk, comprising regions of instability that contain international terrorism threats and significantly increase business risk exposures in adjacent areas. Pockets of severe risk stretch

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



74%

of corporate treasury and finance professionals say their organization

SUFFERED FROM PAYMENTS FRAUD LAST YEAR.

70%

say their organization has implemented controls to

PREVENT BUSINESS EMAIL FROM BEING COMPROMISED.

“Business leaders need to equip their people and systems with the tools and resources needed to prevent fraud and alleviate the impact of an attack,” says Jim Kaitz, president and CEO of the Association for Financial Professionals.

Source: Association for Financial Professionals, 2017 AFP Payments Fraud Survey

across portions of northern Africa, the eastern Mediterranean, and South Asia.

Oil and gas companies were the target of nearly half of all attacks on commercial interests in 2016. Nigeria and Colombia topped the list of countries affected by such attacks.

“Global politics in 2017 is moving in a more violent and crisis-prone direction,” says

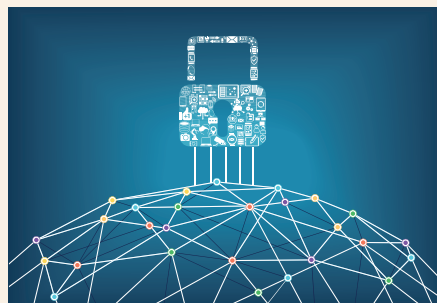
Henry Wilkinson, head of Intelligence and Analysis at The Risk Advisory Group. “In 2017, businesses must develop strategies to face more business-threatening risks from the geopolitical realm. Authoritarian nationalism is on the rise and with it the risks of interstate crises and conflict, coups and rebellion, as well as political risks.” — **D. SALIERNO**

IMPROVING GLOBAL SECURITY MEASURES

Banks now must self-attest to new SWIFT cybersecurity standards.

In the wake of bank cyberattacks in the last year, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) has released security standards via a Customer Security Controls Framework that banks must comply with by the end of 2017 and then annually. SWIFT is the primary communication platform for more than 11,000 banks in 200 countries.

SWIFT has faced pressure to strengthen its cybersecurity measures after hackers exploited the central bank of Bangladesh’s system to steal \$81 million in 2016. The new controls include detailed requirements to physically isolate SWIFT-related equipment, protect access to tokens containing SWIFT credentials, and have a cyber incident response plan.



In January 2018, the compliance status of banks will be available to their counterparts, allowing for transparency and the ability to assess the risk of doing business with them. SWIFT will also begin reporting banks that don’t comply with the new standards to regulators.

— **S. STEFFEE**

LEADERS SET WRONG ETHICAL TONE

Lack of executive action influencing attitudes toward corruption.

Most respondents say corrupt business practices happen widely in their country, and nearly half have considered resigning over unethical conduct,

according to EY’s Europe, Middle East, India, and Africa (EMEIA) Fraud Survey 2017 of 4,100 employees



from large companies in 41 countries. Moreover, while 52 percent of respondents have had information or concerns about misconduct in their company, 48 percent of them have felt pressured to keep silent.

“Often companies sit on unreported conduct, playing the odds game, reasoning that the Serious Fraud Office won’t find out,” Hannah



Visit InternalAuditor.org to read an extended interview with Pilar Caballero.

von Dadelszen, joint head of Fraud with the U.K. Serious Fraud Office, says in the survey report. “That seems to me to be a risky and unpredictable analysis, given the world today.”

Attitudes toward unethical behavior are more relaxed among the young generation, the report notes. Seventy-three percent of Generation Y (25 to 34 year olds) respondents say they can justify unethical behavior to help a business survive. One-fourth of Generation Y respondents say they would offer cash payments to win or retain business, compared to only 14 percent of all other surveyed age groups.

Generation Y also has low standards for management and co-workers. Most (68 percent) report their company’s executives would act unethically for business reasons, while 49 percent say their colleagues would do so to advance their career.

Such findings suggest that company executives and boards aren’t setting the right ethical tone, with 77 percent of director and senior manager respondents saying they could justify unethical behavior to help the business survive. “There is worrying evidence of a lack of leadership from senior executives to tackle bribery and corruption,” says Jim McCurry, EY EMEA Fraud Investigation and Dispute Services leader, “which may be negatively influencing the younger generation workforce.”

— CLAUDIA GESIOTTO

THE CULTURE IMPACT

Tone at the top and visible support from management are crucial in shaping the organization’s ethical values, says Pilar Caballero, chief compliance officer at Ryder Systems.



How can a board or management best change a toxic culture or nurture a positive culture? While the board has oversight of the alignment of the company’s culture with its strategic vision, it is difficult for a board to directly shape corporate culture. Management is in the best position to impact culture. The tone at the top and management’s visible support of a compliance and ethics program are crucial. For example, how management responds when its most beloved, top-performing employees misbehave sends an important cultural message as to what is tolerated and the collective values of the organization.

Is culture always to blame for misconduct? While culture is frequently a significant factor when misconduct occurs, culture is not always the only culprit. Rogue employees can behave poorly, contrary to company culture, and create liability for companies. How a company reacts to misconduct by an employee or group of employees can say a great deal about the company’s culture and goes a long way toward cultivating the right tone. Leveraging information and resources from internal audit, human resources, finance, and legal helps keep a pulse on the culture.

DEVICES RAISE LEGAL WOES

The proliferation of personal activity increases discoverable data on networks.



Sixty percent of employees in the U.S. say they have connected to their organization’s Wi-Fi network using personal devices to send personal email, send text and instant messages, and post on social media, according to a Harris Poll survey

of more than 1,000 respondents sponsored by e-discovery software company kCura.

All this personal activity is greatly increasing the data that is potentially discoverable in a lawsuit or regulatory action, subjecting organizations to potential sanctions, the report notes. A 2016 Osterman Research study found that organizations store a mean of 49 gigabytes of email data per user.

Having a clear data retention policy can help organizations, but 63 percent of respondents say they don’t know whether their organization has policies on email retention or checking personal email at work. Seventy percent use inbox folders to file information. “When corporations don’t take the steps to govern their information... they could face an array of legal headaches, IT frustrations, and high costs,” says David Horrigan, e-discovery counsel at kCura. — T. MCCOLLUM

CIA[®] EXAM PREP FROM THE CIA EXPERTS



Achieve exam day excellence with The IIA's CIA Learning System[®]

- **Learn** the entire global CIA exam syllabus in a concise and easy-to-understand format.
- **Create** a customized SmartStudy[™] plan based on your areas of strength and weakness.
- **Study** on-the-go with interactive online study tools that are optimized for your mobile device.

For more information or to create your free study plan, visit www.LearnCIA.com.

 **The Institute of Internal Auditors**

Back to Basics

BY SETH DAVIS EDITED BY JAMES ROTH + LAURA SOILEAU

KEY STAKEHOLDER SURVEYS

Internal auditors should look to get feedback from their most important customers.

Requirements for a quality assurance and improvement program (QAIP) are outlined in IIA Standard 1300. An integral part of any QAIP should be to help ensure an internal audit department is addressing expectations through the use of surveys. However, audit departments often limit the use of surveys to management in the area in which assurance or advisory activities are performed and miss an opportunity to obtain feedback from other key stakeholders, including the audit committee and executive management.

Management Surveys

Audit departments should have a process to survey management at the conclusion of assurance or advisory activities to help identify opportunities for improvement. Questions should be objective and geared toward adherence to the *International Standards for the*

Professional Practice of Internal Auditing to help minimize subjective responses. In addition, rather than asking “yes” or “no” questions, respondents should be provided a scale ranging from “strongly agree” to “strongly disagree” or a number range such as 1 through 4. Including space to write comments to further elaborate on each of the ratings will provide greater insight into management’s perspective.

Just as action is expected by audit clients when control concerns are noted from audits, the chief audit executive (CAE) should take action if the response from a survey question falls below established expectations. For example, any score that is less than 3 on a 4-point scale should result in a follow-up. The process may include contacting the respondent or head of the area to obtain further information and reiterate the department’s commitment to quality. Action may involve updating

a department manual as well as communicating existing or enhanced procedures to all auditors to help avoid shortcomings in the future.

In addition, survey results should be shared with the audit committee and executive management as part of a balanced scorecard to measure the department on the basis of cost, quality, and timeliness. Survey results can be an effective measurement of quality for the department and should be paired with other quality metrics.

Despite efforts to create objective questions, it is often difficult to avoid correlation between the audit opinion rating and the survey results. It is common for audits with satisfactory ratings to receive high opinion scores while audits with unsatisfactory ratings receive low survey scores despite efforts to adhere to department policies and the *Standards*. Management is human and may use the survey as an opportunity to



VISIT
[Internal Auditor.org](http://InternalAuditor.org)
for a list of
assurance &
advisory service
questions.

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



KEY STAKEHOLDER SURVEY

Statements should be ranked and opportunity for comment provided.

- » Internal audit is independent and objective in performing its work.
- » Internal audit possesses the knowledge and skills, such as insurance industry knowledge and technology skills, needed to perform its responsibilities.
- » Internal audit understands company business operations and strategy.
- » The audit plan is risk-based.
- » I receive adequate updates on the progress of achieving the audit plan.
- » Internal audit evaluates risk exposures and the adequacy and effectiveness of related controls regarding:
 - » Achievement of strategic objectives.
 - » Reliability and integrity of financial and operational information.
 - » Effectiveness and efficiency of operations and programs.
 - » Compliance with laws, regulations, policies, procedures, and contracts.
 - » Safeguarding of assets.
- » Internal audit adequately assesses and provides appropriate recommendations for helping improve the governance process at the organization, including:
 - » Promoting appropriate ethics and values within the organization.
 - » Ensuring effective organizational performance management and accountability.
 - » Communicating risk and control information to appropriate areas of the organization.
 - » Coordinating the activities of and communicating information among the board, external auditors, and management.
- » Internal audit reports and communications are clear, accurate, and issued timely.
- » The conclusions reached in audit reports and the opinions rendered are appropriate.
- » Internal audit shares information and coordinates activities with other internal and external providers of assurance and advisory activities to ensure adequate coverage and minimize any duplication of efforts.

praise or criticize the audit team, regardless of how the team actually performed.

Key Stakeholder Surveys

Managers over the areas where assurance or advisory activities are being provided are not the most important customer of the audit. First and foremost, internal audit serves the needs of the audit committee, followed closely by executive management. To ensure it's meeting key stakeholder needs, the department should have a mechanism in place such as a "Key Stakeholder Survey" (see on this page).


By surveying key stakeholders, the audit department can assess whether it is addressing Standards 2010: Planning, 2110: Governance, 2120: Risk Management, and 2420: Quality of Communications. The audit committee and executive management are in the best position to provide insight into the effectiveness of the department in addressing these standards as they consider the overall audit plan and results communicated throughout the year. While survey questions related to these standards can be asked of management over each audit area, key stakeholders see the broader value audits bring to the organization as a whole.

Using another department such as Communications or a third party and making the survey anonymous will

improve the chances that key stakeholders will be more candid. Survey results should be shared with the audit committee, executive management, and external audit. Scores that are less than desirable, or comments that may indicate improvement opportunities, should be discussed along with action plans. These plans should be tracked with progress reported periodically to the audit committee and executive management.

Create a Repeatable Process

Performing key stakeholder surveys regularly, ideally annually, helps the CAE more quickly identify areas of concern rather than waiting for them to surface as part of an external quality assessment review or, worse yet, from complaints that may go to the audit committee regarding the department.

While many management surveys are performed at the conclusion of each assurance or advisory activity, these surveys may not provide feedback from the most important group of customers. Departments should create a repeatable process to survey the audit committee, executive management, and external audit and incorporate this into their QAIP. 

SETH DAVIS, CIA, CPA, CFSA, CISA, is vice president of internal audit at RLI Insurance in Peoria, Ill.

The Society of Corporate Compliance & Ethics 16th Annual

Compliance & Ethics Institute

October 15-18, 2017 • Caesars Palace • Las Vegas, NV



Join us in Las Vegas!

- Follow a track: ♦ Risk ♦ Ethics ♦ Compliance Lawyer
♦ Case Studies ♦ General Compliance/Hot Topics
♦ Multinational/International ♦ Investigations Workshop
♦ IT compliance ♦ Advanced Discussion Groups

150+
SPEAKERS

8 LEARNING
TRACKS

100+
SESSIONS

Register by June 19 to save up to \$575

Learn more and register at complianceethicsinstitute.org

APPLICATION CONTROL TESTING

Control reviews can help ensure critical software applications function effectively and securely.

Computers, servers, laptops, tablets, smartphones—these are all hardware devices that have connectivity. However, they do nothing without software. Applications are what enable people to work with technology devices and allow them to connect and communicate with other devices.

Internal auditors need to be aware of what applications are being used when they audit a process. In fact, with the reliance being placed on applications in every business area, auditors are not performing a complete audit if they don't address the controls within those applications.

Controlling Applications

Application controls encompass every feature and function of the application and will depend on what the business area does, what the application is, and how much the area relies on the application. To identify

them, internal auditors must ask process owners: What are the primary objectives for this area? What tools are used to help meet those goals? What types of reviews are performed? These questions can help auditors narrow their focus to the key aspects of the application.

Having identified the key application processes, auditors need to identify the controls that are in place. The IIA's Global Technology Audit Guide (GTAG) 8: Auditing Application Controls breaks down application controls into input, processing, output, storage, and monitoring. The responsibility for these controls is shared between the business and IT, so auditing them should be based on an integrated audit approach. This can be a team with finance, operations, and IT auditors, or it can be an auditor who is familiar with business and IT functions.

Auditors should identify all of the controls in the

application so they can risk-rank them and prioritize their testing. A framework such as the one described in GTAG 8 can help guide this effort.

Input Controls

Controls such as "edit checks" are usually built into the application, but some input controls can be configurable, such as duplication checks and access controls.

Built-in Controls Auditors may not have to test controls such as field definitions (users can't substitute an "o" for a "0" in a numeric field) if they are considered low risk. If they need to be tested, auditors need to validate that they exist because no change they implement will alter such controls.

Configurable Controls

When auditors look at configurable controls, they also need to look at the controls over the configuration. Who can make changes and how

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



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

are they tested? Look into the configuration settings for the higher-risk controls. Which roles permit data entry versus only data view? Are there role combinations that are prohibited? These parameters are often defined in configuration files that can be viewed and modified.

Processing Controls

Another major aspect of application control testing is looking at the processing controls. The internal processing is the reason why the application exists, and it might be justifiable to think the controls over processing are low-risk areas. However, the processing controls may not be as accurate as auditors would like, and changes to the software as it is updated may have an impact on the processing

Auditors should check local procedures to ensure overrides have limitations.

controls. The best way to address these concerns is to look at some of the key processes.

Critical Calculations Discuss any critical calculations with the business owner. Are they performing a manual check or reconciliation? If so, have they ever found an error? If there is still a concern, determine whether there is an application user group where additional details on the internal processes might be available.

Custom Calculations Identify any custom calculations that have been incorporated into the application. Because this introduces another potential source of errors, internal auditors should determine who can create custom codes and assess how they are tested. Some custom calculations may be a low risk. For other calculations, especially where the skills to review code might be lacking, the risk may be high or unknown.

Configuration Settings Some processes have mandatory checks, approvals, and thresholds, but some applications allow these controls to be overridden. If this is the case, internal auditors should look at the configuration settings to identify whether what is allowed is also compliant with the procedures. Also, check the local procedures to ensure that overrides, if allowed, have procedural limitations.

Interface Controls

If the application receives its data from another application, or if it sends results to another application, then auditors

should review the interface controls. These are a special case of input and output controls.

Error Detection The file transfer process should include the error detection from the data packets of the network protocols (Open Systems Interconnection (OSI) layer 3), so if the file was sent directly, auditors can be fairly confident that the data was sent or received. But if a less secure protocol is used for the transfer, inquire whether there are other controls such as check sums and record totals that can be used to confirm the data received is complete.


API Limits For many applications, internal auditors also can look into the application programming interfaces (APIs) that are being used. APIs define the interface between the application layer and the transport layer (two more OSI layers). Auditors can look them up online to determine whether there is a risk of data corruption or data leakage. Depending on the application, there also may be issues with bandwidth or timing that the API requires to ensure the application functions appropriately.

Additional Controls

Many other aspects of application control testing can be incorporated into an audit. Before auditors finalize their audit plan, they should consider these aspects of control to ensure they have identified all the highest risks:

- Output controls look at the destination of the application output.
- Storage controls focus on the database structure on which the application relies.
- Monitoring controls look at access logs, input and output file transfer logs, and super-user access.
- Configuration management addresses the procedures surrounding updates to the configuration of the application and its supporting database and operating system.
- Change control and patch management look at how changes to the application are tested and implemented.

Work With Business Owners

Because applications are critical to businesses, application controls represent a risk that internal auditors should test. Auditors should discuss the process, the applications, and the controls with business owners to reach a consensus on the high-risk areas and focus internal audit's efforts. 

RICHARD B. FOWLER, CIA, CRMA, CFE, CISA, is senior audit specialist with Huntington Ingalls Industries in Newport News, Va.

Risk Watch

BY LYNN FOUNTAIN EDITED BY CHARLIE WRIGHT

THE RISK IN THE CONTROL ENVIRONMENT

Auditors need to think beyond check boxes to provide assurance that control processes are addressing risks.

The control environment was not routinely discussed in executive or board discussions before the U.S. Sarbanes-Oxley Act of 2002 was enacted. Since that time, auditors have focused on evaluating the existence and execution of elements of the environment. Most discussions reflect how a positive control environment can strengthen the organization's overall culture and ethics program. However, it can also be viewed in reverse—what risk does a poor control environment bring to the organization?

“Tone at the top,” “management philosophy and operating style,” and “segregation of duties” are phrases commonly used to describe the control environment. These attributes are difficult to measure accurately. An environment that is not effectively evaluated, measured, and monitored may spawn many unacceptable internal and external risks.

As if the risk of an improperly functioning control environment is not enough, the concept is complicated when internal auditors attempt to communicate control environment weaknesses to management. Many organizations rely on questionnaires and anonymous surveys for their assessments. Organizations must proactively peer through these techniques and evaluate the overall transparency of their assessment methods.

The subjective, non-transaction-oriented nature of the control environment creates many challenges. Organizations establish policies, but as changes occur, those policies may no longer be effective. The control environment changes, as well. To address the risk of a poor control environment, organizations must evolve their assessment methods.

Tone at the Top

An organization's tone is often interpreted as the tone

conveyed by senior leaders. This makes evaluation a political hot potato. It can be perilous for internal auditors to advise management that certain actions may not be “setting the right tone.” Yet, to address the risk appropriately, auditors must provide assurance that the policies management has put in place are executed effectively.

For example, Acme Inc. maintains an authorization policy for procurement professionals. On the surface, this appears to contribute to a strong control environment while mitigating the risk of conflict of interests. However, what if the policy does not cover strategic areas such as contract approvals, management overrides, and monitoring methods? Also, assume the policy was created strictly by the finance organization. Taken in the aggregate, each of these factors could create risk to the control environment.

This situation creates a dilemma. How should these

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



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

risks be communicated to management? What if issues are communicated, but management concludes the gaps are not significant concerns? Management's basis for this conclusion may be that no actual problems have been identified to date. To address the risk appropriately, auditors must ask, "If an issue has not yet come to light or been identified, should that fact minimize the finding?"

What if the auditor's opinion of the gap's severity differs from management's opinion? Organizational leaders may push back if they receive a poor control environment assessment. An obvious step for internal auditors may be to speak to the audit committee, but this can be challenging. It may be difficult to communicate a control environment gap to an audience that has been preconditioned by management's view.

To resolve these dilemmas, auditors can:

- Ensure they have authority to analyze and communicate the situation beyond just the existence of policies.
- Ensure management understands the difference between a control gap and a control failure. It is important to know whether the gap has created a failure, but just

Review the potential liabilities to management for improper attestations.

because it hasn't failed to date should not minimize the impact of the gap. The inability to recognize this cause-and-effect relationship will put the control environment at significant risk.

- Encourage independent communication with board members. If management and the auditor disagree about the severity of the issue, the board must be open to both sides of the argument.

Management Philosophy and Operating Style

Philosophy and operating style include how management executes its day to day responsibilities and the manner in which executives provide overall direction. Consider an example of quarterly attestations and their impact on the control environment. U.S.-traded companies have procedures in place for affirmation of internal control processes for Sarbanes-Oxley Section 302. These procedures often involve business-unit managers providing personal subcertifications on controls for their areas of responsibility.

Assume the procedure for quarterly attestations was established several years ago. The subcertification states: "To the best of my knowledge, internal control procedures and financial information within my area of responsibility are accurate

and complete." The certification was originally accompanied by specific training for the business-unit leaders.

Fast forward several years. Many personnel signing the attestations are individuals who have been promoted into new positions but have not been trained on the attestation requirements. New management views the process as a "step" they must complete each quarter because of compliance requirements. If the auditor assumes the standard process of attestation is effective, there may be a risk to the control environment. Because the attestation is a simple signature, the risk exists that management is simply following a legacy process and does not understand the need for disclosure controls. One solution is to review the Sarbanes-Oxley requirements and potential fines and liabilities to management for improper attestations. Outlining the risk may convince management to re-evaluate and solidify the process.

Segregation of Duties

A strong control environment can only be supported through appropriate segregation of duties. Segregation of duties assist in mitigating the potential for one person to maintain control over an entire process, thus having the opportunity to perpetrate some undesirable behavior. When evaluating the sufficiency of segregation of duties, internal auditors examine responsibilities around transaction authorization, recording, custody of asset, and reconciliation.

Depending on organizational resources, it may not be possible for the organization to fully implement appropriate segregation of duties. In this situation, auditors must assess the risk embedded in the processes, attempt to quantify the risk, communicate to management their observations, and provide alternative methods in which management can monitor transaction activity or provide additional checks and balances for the process.

A Thorough Assessment

The control environment is the foundation upon which an organization can effectively execute strategy. If management focuses only on "check the box" activities, it will miss critical attributes that may result in major gaps that ultimately impact the organization's viability and control environment. That is why it is important for internal auditors to fully assess gaps or flaws and provide adequate assurance regarding the sufficiency of controls.

LYNN FOUNTAIN, CGMA, CRMA, is a business consultant, author, and trainer with Fountain Consulting and Training Services in Overland Park, Kan.

Fraud Findings

BY GRANT WAHLSTROM EDITED BY BRYANT RICHARDS

THE “FREE TRIAL” SCAM

Data analytics uncovers a sales force fraud using prepaid credit cards to boost commissions.

“I specialize in high-crime, low-income areas, where the average household is on government assistance.” These were the exact words of Erin Turner, one of the top sales representatives at a home security company who was now under investigation for fraud. Bruce Dwyer, the company’s forensic auditor, sat baffled by the comment, wondering how so many people living on government assistance could afford a home security and automation system with a \$50 monthly monitoring fee. During the interview, Turner produced a purse full of prepaid credit cards and explained to Dwyer how she obtained them, what they were used for, and how she provided the numbers to some of her customers to facilitate installation of a security system.

Dwyer’s investigation was the result of an analysis of a national summer promotion. The premise of the

offer was a limited time, deeply discounted installation with a three-year monitoring agreement. The marketing analysis had produced mixed results. The company had made a lot of deeply discounted sales but many of the units were already being discontinued for nonpayment. Some of the sales representatives had disproportionate disconnect rates. Management suspected fraud. Dwyer was tasked with conducting the investigation. He decided to start with what appeared to be the largest offender, Turner, who also happened to be one of the top sales representatives.

Turner built her book of business using the company’s promoter program, where sales representatives are encouraged to develop a network of professionals and small businesses — promoters — that would refer potential customers to them. If a referral turned into a sale, the sales

representative earned a commission and the promoter earned a referral fee. Turner was working with one primary promoter in a handful of large apartment complexes. A quick review of her personnel file revealed the promoter to be Turner’s sister.

During the interview, Turner told Dwyer that her sister was going door to door and convincing the neighbors to install a security system. Her sales pitch was that the system was free to install, they could try it for six months without making a payment, and if they were not satisfied with the service they could simply stop making payments. There were no strings attached. Turner’s sister provided customers with a prepaid credit card to get the installation completed.

On Dwyer’s flight home, he made a list of all the sales representatives and wondered if they also were abusing prepaid credit

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



TO COMMENT on this article,
EMAIL the author at grant.wahlstrom@theia.org

cards. A prepaid credit card is activated when the cardholder pays a small fee and “loads” the card by putting a set amount of money on it. Once a prepaid credit card is activated, the number is live until the card’s expiration date or the holder cancels the card. When a transaction occurs, the balance on the card is reduced. Dwyer discovered that the company’s billing and collection system could only validate that a credit card presented was “live.” In other words, the system could not determine if the credit card presented for installation charges and recurring payments was a credit card, gift card, or prepaid credit card. Furthermore, if it was a prepaid credit card they

The scheme was costing the company almost \$5 million annually.

could not validate that enough funds were available for the installation charges, let alone the recurring monthly monitoring fees.

As luck would have it, Thomas Border, the IT specialist responsible for credit card transactions, had noticed a pattern of abuse with prepaid credit cards. Together, Dwyer and Border analyzed all credit card transactions for a six-month period to identify and quantify a pattern of abuse. To conduct the investigation, credit card transactions had to be matched to a bank identification number (BIN) database to identify prepaid credit card usage. The 16 digits on credit cards are the result of a complex algorithm. The first six digits are referred to as the BIN. The BIN can determine what institution issued the card and the type of card it is. Dwyer and Border obtained the customer account numbers associated with the cards and the names of the sales representatives who made the sales to identify who had either provided or accepted prepaid credit cards.

Based on the findings, Dwyer then conducted investigations of the other sales representatives and discovered a similar pattern of abuse. In some cases, Dwyer identified sales representatives who signed up 25 to 30 customers on a single prepaid credit card. Most of these accounts would immediately default on their payments, but the sales representatives collected commissions on each sale, regardless. At one point, Dwyer estimated that the scheme was costing the company almost \$5 million annually over the course of two years. The sales representatives involved in the scheme were immediately terminated.

Lessons Learned

- ➔ Prepaid credit card usage is a common fraud scheme among commissioned sales forces, so internal auditors should compare all credit card transactions against a BIN database to identify prepaid credit card transactions, find out which customer accounts used a prepaid credit card as payment, look at the payment history while focusing on customers who have made zero or a single payment, and identify the sales representatives on the account to uncover any wrongdoing.
- ➔ The many-to-one test identifies how many customer accounts are associated with a single credit card number. After identifying a target list, internal auditors should look at the customer content (name, address, and location) to see if they are family members or small businesses that might be legitimately sharing a credit card. If no commonality can be identified, internal auditors should investigate. Incidentally, this procedure also works for checking accounts.
- ➔ The scheme could have been caught sooner if the finance department was working more closely with the company’s credit card processor. Processors can assist with identifying prepaid credit cards in their transaction database.
- ➔ Companies can decide not to accept prepaid credit cards for recurring monthly payments, but it must first check its agreement with its credit card processor as it may be legally required to accept prepaid credit cards as a form of payment.
- ➔ Exception reports identifying sales representatives accepting prepaid credit cards should be produced monthly and distributed to area general managers to review for fraudulent activity. Internal audit should be notified of any apparent fraudulent activity and engaged to conduct an investigation.
- ➔ As a result of this investigation, and several other observations, the company began conducting enhanced customer screenings in the form of credit checks on all prospective customers. Customers who have low credit scores are now required to make several months of recurring payments before system installation can occur. Requiring several months of recurring payments up front helps reduce fraudulent use of prepaid credit cards.

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



San Diego Schools Approve Plan to Gut Internal Audit Department

UNDER SIEGE

ed HISD Chief Auditor:
district does not want the
irt to be published'

er Auditor Sues

IS Over Firing

of

contracting

chdog ...

It Barks

Public sector auditors can face intimidation, isolation, retaliation, suspension – even termination – just for doing their job.

Russell A. Jackson

In 2016, the Houston Independent School District's Board of Education suspended all of Chief Audit Executive (CAE) Richard Patton's duties for "misconduct and other performance concerns" — according to the board's public explanation. An outside attorney investigated what Patton points out is "a frivolous claim that I used district resources to scan approximately 10 pages of personal documents over a period of roughly two years." Despite numerous requests to release the results of the investigation to the public, the district has not done so. After the

investigation, Patton returned to work, but he says his duties and responsibilities were "diminished by the board in a number of ways." Just before the suspension, his team worked on several internal investigations and cooperated with the U.S. Federal Bureau of Investigation and district attorney on matters those agencies had initiated. Because of what he calls clear retaliation and the reduction of duties — which, he notes, "seriously impacted the district's audit charter and my team's ability to comply with The IIA's Code of Ethics" — he took legal action.

The sad reality is that public sector auditors can face retaliation — isolation, smear campaigns, diminution of duties, even suspension and termination — just for doing their jobs. If the fruits of the audit function's labors conflict with an agency head's political agenda, too often the political agenda wins and the auditor loses. The threat is so real, and the stakes so high, that many practitioners embroiled in sticky political situations have to inform their colleagues anonymously — or with the approval of a lawyer. That's why Patton's tale is attributed directly to him; all his comments have been approved by counsel so they don't impact the ongoing litigation.

Solutions are few, but they do exist. If other practitioners know what to watch for and how to prepare for the worst, some may avoid the untenable situations their colleagues deal with. As an internal auditor under fire at a mid-level school district says, "Exposure of these issues may help someone else." Ultimately, of course, some public sector auditors caught up in politics will simply have to fall on their swords. At the end of the day, the public servant trying to suppress the truth likely won an election or received an appointment from someone in office, so the auditor trying to tell the truth may be pressured to get on board or get out. But in many cases, targeted relationship-building and a firm grasp of the agency's governance structure will go a long way toward avoiding catastrophe.

POLITICAL MOTIVATION

The political motivation to punish an auditor often involves information that's incriminating to the person who ordered the audit in the first place — sometimes under a law or regulation. In one case, an audit investigation found evidence that a school board CEO had been less than honest about his credentials; in another, a culture audit — which, in law enforcement is often going to be politically sensitive — contained pretty damning results; and another uncovered fraud in a university's program accepting bodies of people willed to science. Often, it's a more mundane reason, like auditors looking into contracts or programs that executive directors don't want exposed or, as in Patton's case, assisting outside agencies in



their investigations. Sometimes it’s as simple as an executive director who insists that the audit function in general has a “gotcha” mentality. In fact, one anonymous practitioner facing retaliation at a local school district says she has come to believe that “any audit that falls under the chief operating officer or chief financial officer’s (CFO’s) jurisdiction or any audit that makes a board look like it isn’t providing governance and oversight will be political.”

The means of punishing auditors vary as well, within fairly defined limits. The mid-level school district auditor reports to a superintendent who always threatens termination. There are also common reports of campaigns to discredit CAEs who ruffle the wrong feathers—including suspiciously conducted reviews of their performance—and practitioners being isolated, often by “people who were friendly a year ago,” as the mid-level school district auditor puts it, adding, “Maybe they’ve been told they need to stay away from me to protect themselves.”

Retaliation also often includes reduction of duties. Patton notes that the ethics and compliance function was totally removed from the CAE’s duties, and the audit management team received correspondence from the district’s lawyers to cease existing investigations. Patton says he also received a

letter stating that work activities outside of the audit plan must be approved by the whole board before beginning.

Other auditors report not being allowed to fill vacancies and being ordered to stop conducting operational audits. In some cases, the audit plan is even pulled from the board’s agenda, executive leadership makes sure discussion is delayed or disrupted, or management and board members cease regular communications with the audit department. Auditor Steve Goodson was once in an all-too-familiar situation: A CEO at “a major Texas state agency” told him on the first day on the job—after he was hired by the board—that if he wanted to work there, he was to accept instructions only from the CEO, regardless of what the board instructed him to do. “He often directed which areas of the organization I would not be allowed to audit,” Goodson recalls. “These were some of the same areas the board had instructed me to audit, so I was in a tight spot. For four years, I worked hard to navigate and negotiate an appropriate path for the audit function.”

DUE PROCESS

Sometimes the retaliation is more subtle, and never really impacts the auditor. Kip Memmott, audit director for

“I believe what I faced may appropriately be defined as retaliation.”



One of the top reasons **76%** of public sector auditors **do not** audit **culture** is because of lack of support from executive management, according to The IIA's 2016 Global Pulse of Internal Audit.

“They forbade me to do any work, and things have been at a standstill for six months. I think most internal auditors in my situation would have already quit.”



the Oregon Secretary of State's Office, once worked for a county government body where he conducted a performance audit that, he reports, unearthed a lot of problems. The CFO he reported to didn't want to ruffle any feathers, but told him to proceed if he wanted to and the problems would be fixed, but the report wouldn't be issued. "I felt like my standing fell and communications were superficial from then on," Memmott says. The happy ending was that the CFO departed soon after.

Mike Peppers, on the other hand, reports he has not "been in a situation in my 25-year career where I've had pressure to suppress something in a report." The CAE at the Austin-based University of Texas System credits that mainly to his perception that public sector political retaliation "is a little less likely because so much of what we do is public, and it has been said that sunshine is the best disinfectant." Much of his output is public record, he explains, and audit committee meetings are broadcast live on the internet. "My colleagues in private companies have trouble wrapping their heads around that," he quips.

Peppers does, of course, recognize that political challenges exist. He recommends developing strong relationships

with audit committees so they "completely understand the role of internal audit and realize the responsibility they have to encourage an open and ethical environment." That may be in the agency's or department's charter, and if it's not, the CAE needs to drive it, he urges.

"CAEs need to recognize the important elements of protection, and know their limits within them, so if a situation arises, they are prepared to have those tough conversations," Peppers says. "The first conversation should not take place when there's a problem." Similarly, auditors should know the process for removing a CAE. "No one would want to make excuses for a bad CAE," he says. "Any time a CAE needs to be removed, there needs to be a strong process in place for the action to be reviewed in the sunshine to make certain there wasn't anything inappropriate" in how the termination was handled. While it's probably the audit committee's responsibility to ensure that's the case, new internal audit hires should make sure, when they come into the role, that the process is clear.

Auditors who've been burned by political pressure agree. "It starts in the interview process," the county-level school district auditor says. "I wasn't told the truth when



I interviewed. I should have been more cautious and said it was a deal breaker if I didn't talk to the board. You have to square all of that up before you start. Once you're hired, you don't have a whole lot of places to go for help." That anonymous auditor adds that you should definitely establish boundaries at the interview and make sure to vet the reporting structure at the place they're going to work—and to walk away if you're not comfortable. If you're deceived, it's a tough place to be. For his part, Patton even advises negotiating a contract that allows the audit department to have its own outside attorney.

FORGING RELATIONSHIPS

Once on the job, all auditors should build relationships with the people with whom they work, Memmott advises. Start by winning over staff, he suggests, to "learn who they are and get a feel for trends. Meet your colleagues, understand what they're working on and the context they're working in." That should be clear from governance documents. Internal auditors should then use that insight to shore up potentially troublesome relationships and make sure the governance documents that define the internal audit function are known to, and understood by, everyone. Don't assume anyone has read your charter, Memmott warns. "Try to make sure everybody is on the same page when something happens." Take a look at past audit reports, too, he suggests. What do they look like? What have the responses been? Has there been a high level of agreement or disagreement? One sign of trouble, he notes, is terminated audits or bad or no responses to them.

Internal auditors also can improve their chances of surviving a political challenge by maintaining strong communications with management and showing through their work that they value being part of the team, says George McGowan, director, audit services and management support, for the City of Orlando, Fla. "Internal auditors are just as much managers over the quality of city services as those in the operating departments," he says. "We need to demonstrate this level of care when we interact with managers. They need to know that we want the city to be successful in delivering its services and we don't get any pleasure from pointing out flaws and troubles." That doesn't mean shirking duties, he emphasizes. "In the end, that responsibility does fall to us," he notes, "and it is necessary to develop a record of the conditions we find as well as what can be done to change the outcome to a positive."

When crisis arises, and with it the potential for political retaliation against an internal auditor whose revelations may have sparked it, smart practitioners will keep the lines of communication open, Peppers comments. Whenever the

PROTECT YOURSELF

Internal auditors with experience in political challenges offer these additional tips:

- » **Know what to watch for.** "Your first sign of trouble is when you are not provided freedom to conduct sensitive work activities," Houston Independent School District's former Board of Education Chief Audit Executive Richard Patton says. And an anonymous local school district auditor points to "a lack of communication, such as no or delayed responses to requests to meet or to provide documents" as a sign that trouble could be brewing.
- » **Watch the tone of a report when drafting it.** "You can change two or three words in the header and not change the report," Kip Memmott, audit director for the Oregon Secretary of State, says.
- » **Document, document, document. Verify, verify, verify.** George McGowan, City of Orlando's director of audit services and management support, urges thoroughly discussing each issue with the parties involved to understand the root cause. "Every engagement needs care and feeding," he says. "Those being audited need to feel directly involved in both understanding and then resolving the issues."
- » **Make sure that any time an audit involves criminal or fraudulent findings the appropriate authorities are brought in.** Indeed, any time a situation becomes controversial, bring another auditor to take notes.
- » **Create a paper trail.** This will back up your findings and the way you present them.
- » **Understand that going to the media has serious repercussions.** Memmott states, "Going to the media will not protect you. In fact, it will backfire."
- » **Have a thick skin.** Auditor Steve Goodson advises, "Try to understand the situation from the many various perspectives. Be as flexible as you can."
- » **Hire a lawyer.**

CAE sees that there's going to be an audit that might result in reputational damage, he or she may err, unwisely, on the side of nondisclosure, he explains, adding, "But if the CAE is working with management through all of those times and keeping people informed throughout the process, that's going to help down the line."

“He point blank told me to change the report.
I point blank told him I wasn’t going to.”




Memcott agrees. “Right up front, let people know you’re not here to play ‘gotcha,’” he says, also calling for frequent updates. “If it’s communication overkill, they’ll tell you.” And auditors must do more than simply point out what’s wrong. You have to tell them how you can help them, he urges. “If you can give them real examples, that helps.” And remember that people want to be told when things are working well, too. “If you do a lot of that,” he says, “you can clear out a lot of the conflict.”

Goodson also advises leaning on the *International Standards for the Professional Practice of Internal Auditing* and educating stakeholders about what it means to be an internal auditor and what that means as far as the particular circumstance. Essentially, assure stakeholders that you understand what you’re dealing with.

HARD CHOICES

The sad reality is that public sector auditors who are being victimized by political retaliation oftentimes have no choice but to resign. Says the local school district auditor, “It’s very difficult to make a change if the organization is dysfunctional. Sometimes you can make renovations to a house that will improve the functionality, but sometimes you just have to declare the house condemned and start over.” Memcott

agrees. “I don’t think there is a lot of protection,” he points out, unless the practitioner is a mid-level or higher manager with civil service protection. And even then, he says, “you can make it tough for your boss to get rid of you, bloody everybody, and still lose.” And the bottom line is this: If the agency head is an elected official, the auditor needs to find a new job. It’s the elected official’s domain, but you can choose not to work in that environment. Auditing “requires that courage,” Memcott adds. “It’s a reality of the game. And the higher you go, the more you have to accept that you’re out there on your own.”

Whether a victim of the politics of internal auditing or one who’s avoided that frustration, “Never compromise your principles or do anything illegal,” the mid-level school district auditor stresses. Part of that is learning not to take the treatment personally. “You definitely have to reconcile those feelings and understand that you’re the one doing the right thing. Don’t try to fit in,” that anonymous practitioner in a difficult situation urges. “Otherwise, you make emotional, bad decisions when you need to stay on the right track.” 

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

How to Audit Culture

Culture audits can help practitioners gain insight into the causes of poor organizational behavior.

James Roth

Illustration by Edwin Fotheringham

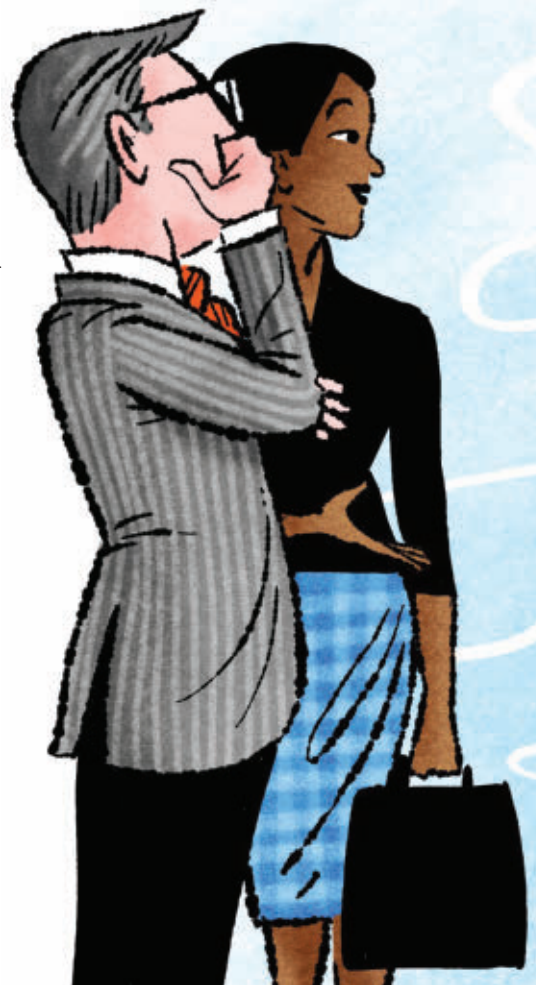
Enron, Worldcom, FIFA, General Motors, Volkswagen, and Wells Fargo are just a few examples of scandals caused by organizational cultures that encouraged inappropriate behavior. The reputation risk cries out for audit coverage, yet only 42 percent of internal audit functions are auditing their organization's culture, according to The IIA's 2016 North American Pulse of Internal Audit study.

Auditing an organization's culture can be challenging because of its complexity, its subjectivity, and the potential resistance of key players. However, approaches and techniques pioneered by some internal audit functions can help auditors successfully enhance coverage of culture.

COMPLEXITY OF CULTURE

One definition of culture is "the actual values that influence everyday behavior within the organization." These are not the organization's stated values or desired values, but the values people actually live by in the workplace. Culture is shaped primarily by tone at the top, but it is also influenced by factors such as business strategy, organizational structure, incentives, employees' personal values, and human resource practices. Each factor interacts with the others in a complex web. Adding to this complexity are:

Subcultures Managers create subcultures within their spheres of influence, which might not be consistent with the organization's culture. This challenge is



an opportunity for internal audit because it can be identified during audits and provide valuable information for higher-level management.

Different Cultures There is no right culture and no ideal risk/reward balance, even for different parts of the organization. For example, finance may have a more conservative culture, and sales may have a more aggressive culture, which is appropriate within limits. To meet this challenge, internal auditors must have good judgment, business knowledge, and transparent communication to put such differences into perspective and determine whether they are appropriate.

No Defined Criteria Ideally, management and the board should define expectations for each part of the business, as well as the observable behaviors that illustrate consistency with, or variance from, that expectation. This is rarely done. The lack of clear, specific criteria to audit against increases the challenge of auditing



culture. To address this challenge, some internal audit departments have developed a culture model—usually starting from a model developed by an outside firm. For example, Prudential uses a model it co-developed with EY (see “Auditing Prudential’s Control Environment: Areas of Focus” on page 33). Once the board and executives buy into the model, internal audit

can describe what they think the culture is, but their perception of the culture is filtered by employees’ unwillingness to tell them there are problems in the culture.

The culture exists in the perceptions of employees. If employees believe the culture is “win at all costs, do whatever it takes,” that’s the way they behave. If employees believe the culture is “put the customer first,” that’s the way they behave. That’s why a common definition of culture is simply “how we do things around here.”

Employees are the best source of information about the culture, but getting that information presents several challenges for auditors:

- » Employees might not be fully candid, especially if they fear retribution for saying something negative to the auditors.
- » They may have cultural blind spots that make them unable to see a cultural weakness from within the culture.
- » Some employees may be chronic complainers.
- » Surveys, interviews, and workshops by internal auditors might be influenced by the same blind spots.
- » The response to the results will be influenced by the culture.

Internal auditors must be aware of these challenges and use knowledge of their organization, good judgment, and interpersonal skills to deal with them as they develop and apply their assessment techniques. There are several keys to auditing culture successfully.

SUCCESS FACTORS

Executives and board members are at least intuitively aware of the challenges in auditing culture and may be skeptical of internal audit’s ability to deal with them. For the audit to succeed, executives and board members must be willing to accept less hard evidence than

Employees are the best source of information about the culture.



can develop audit programs and tools to address specific expectations and behaviors within that framework.

The Extended Organization

Although they are difficult to identify, cultural inconsistencies in global operations, outsourced functions, vendors, and joint venture partners can be harmful to the organization. Internal auditors must adapt their approach, audit tools, and judgment to account for differences in country cultures. Some organizations require their vendors and third-party providers to submit a report annually showing how they comply with the organization’s values. Then they meet to discuss the report, which can be more meaningful than the report, itself.

CULTURE IS PERCEPTION

Before addressing the techniques internal auditors are using to audit culture, a basic principle and its related challenges are worth discussing. An organization’s culture does not exist in formal documents such as codes of ethics or value statements, which only reflect what the organization says it wants the culture to be. Nor does it exist in what the board and executives tell auditors about the

37% of audit functions incorporate **cultural reviews** into their existing engagements, while 8% have a dedicated culture audit, according to a November 2016 study by research firm CEB.

they are used to receiving and accept that there are gray areas (see “The Subjectivity of Culture” on page 35). Chief audit executives (CAEs) must persuade them that their internal audit team has the skills, judgment, tools, and techniques to provide valuable insights into the culture. The team, of course, must in fact have these attributes. If it does and the board agrees, it is helpful to establish auditing culture as a mandate in the internal audit charter. If the team does not have the skills, it is best to take baby steps into evaluating soft controls while building the team toward a more robust focus on culture.

Audit Skills The Chartered Institute of Internal Auditors’ 2016 report, Organizational Culture—Evolving Approaches to Embedding and Assurance, details the

skills and competencies internal auditors in the U.K. and Ireland say the profession needs to audit culture:

- » Professional judgment (84 percent).
- » Use of experienced or senior auditors to lead the work (71 percent).
- » Enhanced communication skills to deliver unpalatable findings (60 percent).
- » Influence and negotiation skills (48 percent).
- » Training from specialists on qualitative methods and survey design (33 percent).

Just 21 percent of respondents say auditors already have the skills necessary to assess culture and soft controls, the survey notes. Organizations could supplement the skills of the audit team

by partnering with other assurance providers, such as those in the second line of defense. Cosourcing with outside providers can be another good option.

Audit’s Relationship to the Business Support from the top is crucial but not sufficient. Internal audit must have earned the trust and credibility of managers throughout the organization to deal with sensitive issues appropriately. If this is not the case, auditors should rely on tools such as anonymous employee surveys initially and focus on building relationships. Extra care should be taken in reporting audit results in ways that are most likely to get corrective action taken without unintended negative repercussions. The CAE and audit managers will have to work more closely with the audit team to be sure they are using mature

AUDITING PRUDENTIAL’S CONTROL ENVIRONMENT: AREAS OF FOCUS





Build a Stronger Team.

Do You Have Your Team Development Road Map?

Meet your current training needs and your future audit team goals with the help of IIA On-site Group Training. We can provide tailored, flexible, and affordable team development plans that focus on your organization's requirements and learning objectives.



Visit www.theiia.org/TeamDevelopment or call +1-407-937-1388.

68% of audit stakeholders in the banking sector encourage culture audits, but only 32% of internal audit functions perform them, according to an IIA Financial Services Audit Center quick poll.

THE SUBJECTIVITY OF CULTURE

Culture is inherently subjective. So how can internal auditors obtain objective evidence about something that is, itself, subjective? The answer is the evidence obtained in auditing culture doesn't have to be as objective as the evidence obtained in auditing hard controls. The applicable *International Standards for the Professional Practice of Internal Auditing* (1100, 1120, 2310, 2320, and 2420) do not require objective evidence. To summarize what the *Standards* say, internal auditors must identify the best attainable information about the culture through the use of appropriate engagement techniques. This information must be factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Internal auditors must base their conclusions and engagement results on appropriate analyses and evaluations. Their reporting of results must be fair, impartial, and the result of a balanced assessment of all relevant facts and circumstances.

To comply with the *Standards*, internal auditors typically use a combination of objective and subjective evidence, evaluate it objectively, and "connect the dots" about the culture in a way that is persuasive. They are careful not to conclude more firmly than the evidence supports, and they present results as giving perspective into the culture rather than stating audit opinions or ratings.

judgment and communicating appropriately with their clients.

SCOPE AND TECHNIQUES

The most comprehensive culture audits combine hard and soft control testing at a variety of levels. For example:

- » Audits of entity-level governance and risk management structures and activities.
- » Audits of processes with significant cultural influence such as ethics training, incentives, and human resource practices.
- » Cross-functional thematic audits such as culture of compliance and management initiatives.
- » Cultural auditing embedded in every audit project.

Audit results should include hard evidence where it applies, as well as the results of interviews and other self-assessment techniques. All audit evidence should be correlated and analyzed until reasonable and persuasive statements about culture emerge. Conclusions should be discussed and modified, if appropriate, at all levels before they are finalized. Internal audit techniques

that have proven effective for auditing culture are root cause analysis, structured interviews, employee surveys, and self-assessment workshops.

Root cause analysis is basic-to-good internal auditing. Pushed deeply enough, the root cause of an audit issue is often cultural. It might be a disconnect between the desired overall culture and the subculture created by a manager. Or it might be pervasive. "Connecting the dots" from numerous audits can create persuasive evidence of an issue in the overall culture.

Structured interviews enable internal auditors to ask a sample of employees the same questions. For example, to determine whether a "culture of compliance" exists in his company, a CAE personally interviews 65 of the 1,000 employees. He starts with simple questions to set each employee at ease and later gets into sensitive questions like, "Have you ever been asked to do anything that you believe violates the code of business conduct or company policies?"

This technique is more objective than unstructured interviews because one set of questions and one skilled interviewer bring consistency to the process. It does, however, require a high level of interviewing skills to detect when someone's positive answer isn't what the person is really thinking and ask the right follow-up questions. It also relies on the interviewer's understanding of what was said and the willingness of upper management to believe its accuracy.

Employee surveys have the advantages of gathering evidence from a large sample of employees and producing objective data. The most common survey technique for internal auditors is asking employees to respond to a series of statements by indicating whether they strongly agree, agree, disagree, or strongly disagree with each statement, with an option like "not applicable" or "don't know" off to the side and not factored into the results. The audit report can then state, for example, that "46 percent of responding employees disagreed or strongly disagreed with the

AUDITOR SPOTLIGHT

Heidelberg Cement and its North American subsidiary, Lehigh Hanson, are global leaders in the cement market. Recently we talked with Anke Eckardt, director of the company's Group Internal Audit (GIA) about their use of CaseWare IDEA Data Analysis software. Here's what she had to say.



Q: What prompted your organization to adopt a data analysis tool?

A: To give you some background, we're a large company that uses three ERP systems that are connected to eight subsystems, most of which can only be accessed by SQL. The reporting on these systems, if any, was very weak and we often received data in PDF format. To make matters more complex, GIA doesn't do financial audits so we don't always have access to the source data.

This environment led us to realize that we needed a data analytics tool. Limited access to data, sampling and interviews alone weren't allowing us to properly quantify issues. It was very frustrating! Because of its intuitive interface and the ability to import any PDF and turn it into a data file, IDEA was our choice.

Q: How has data analysis helped you collaborate with other teams?

A: Data analysis allows my team to think more about the business and its processes. As some auditors know, sales is notorious for designing their own pricing models, so we helped define standards by using IDEA to create a splatter graph of pricing trends by product. There were many unexpected correlations between volumes and prices, which was very interesting to management.

Today we also use IDEA to create monthly VAT (value-added tax) reports

to ensure that the VAT code is correctly assigned on reports to European tax agencies. A similar monthly report is being created for Canada where there is GST, PST and HST (general, provincial and harmonized sales taxes). These reports have uncovered mistakes at the AR and AP level and allowed us to create value by not overpaying on taxes.

Q: What suggestions can you offer to IA teams?

A: Have a dedicated data analyst on your team. It's a huge advantage because they can establish a relationship with IT, making it easier to get the data you need. The data analyst also becomes an expert on the data and—more importantly—can create macros to make analyses repeatable. Because of our analyst, we now have a number of macros stored in IDEA that can be run on defined data sets (or directly from a data extract from IT). You could create similar macros in spreadsheets, but it would take a very long time.

To learn more about how IDEA can improve your audits, visit us at www.casewareanalytics.com.



VISIT InternalAuditor.org to view additional examples of some of the techniques discussed in this article.

statement. ...” This is an objective fact. The auditor then must look for corroborating evidence and investigate the root cause.

A well-constructed survey—provided that employees believe it is anonymous and action will be taken to address their concerns—can generate data that accurately reflects employees’ perceptions of the culture. It is possible, of course, that the results reflect a misperception. This is why the auditor must look for corroborating evidence. If it turns out to be a misperception, that is valuable information that should be reported to the local manager, who can then correct it.

Employee surveys can be used at two levels: on audit projects or organizationwide. Some internal audit departments have a standard survey they use on every audit, with a section in the audit report including corrective action plans. Others develop a survey for just one audit when the situation and level of risk justify the time involved. Some internal audit departments have developed and administer an organizationwide survey, usually annually.

Many large organizations have an existing, organizationwide employee survey. Most of these surveys include little or nothing on topics such as ethics or risk that are essential to the culture. Some internal auditors have reviewed the content, developed survey statements that address these issues, and persuaded management to add them to the survey. They can then use the survey results as a key risk factor in developing their periodic audit plan. When the survey suggests cultural issues in an auditable entity, the results also can be used to help plan and scope that audit. And when process deficiencies are found, the root cause might be identified in the survey. Linking the objectively evidenced deficiency to the survey results can be very persuasive to management that a cultural issue exists.

Facilitated workshops were the first tools used by internal auditors for evaluating soft controls. In this technique, a group of employees is guided through a disciplined analysis, often using the same kind of statements that are used in surveys, together with confidential voting technology to gather and tabulate the results. Discussing the issues that emerge with the employees who experience them can be powerful. Today, workshops are used more by risk management departments for risk assessment, while internal auditors more frequently use surveys.

MATURITY MODEL

Culture does not lend itself to a pass/fail type of audit opinion. IIA guidance addressing sensitive topics often recommends considering a maturity model to report results. With a maturity model, executives and the board can decide how mature they want the organization to be with each attribute listed. Internal audit results can then be presented in terms of the model and help measure how mature each attribute actually is. This reporting vehicle assumes that the organization is working to get better (more mature) with the attributes

Culture might be the most challenging audit topic the profession has faced.

METRICS

In addition to these techniques, internal audit can leverage metrics that reflect the culture to develop the periodic audit plan, plan and scope audit projects, and support audit results. Hard data can be persuasive. A monthly dashboard could give meaningful perspective on the culture to executives and the board. The dashboard could present metrics such as:

- » Customer survey results.
- » Number and trend of customer complaints.
- » Turnover statistics.
- » Sick time statistics.
- » Warranty claims.
- » Frequency of performance targets being missed.
- » Frequency of large projects failing.
- » Hotline statistics.
- » Environmental impact data.

The best metrics auditors can use depends on the organization. Several metrics would be specific to the organization or its industry.

important to it and helps measure progress along the way.

CULTURAL EVIDENCE

Culture might be the most challenging audit topic the profession has ever faced. Internal auditors must be realistic about the constraints they have in their own organizations. If the constraints are substantial, auditors should do what they can at present and look for opportunities to expand over time. It may be impossible to ever give a firm opinion on the quality of an organization’s culture. But good auditors using good techniques, judgment, and communication skills can present solid evidence about the culture to executives and the board. Over time, the picture this evidence paints will become clearer and more persuasive. This may be the most valuable information internal audit will ever provide.

JAMES ROTH, PHD, CIA, CCSA, is author of *Best Practices: Evaluating the Corporate Culture* and president of *Audit-Trends LLC* in Hastings, Minn.



How Agile is your Audit Process?

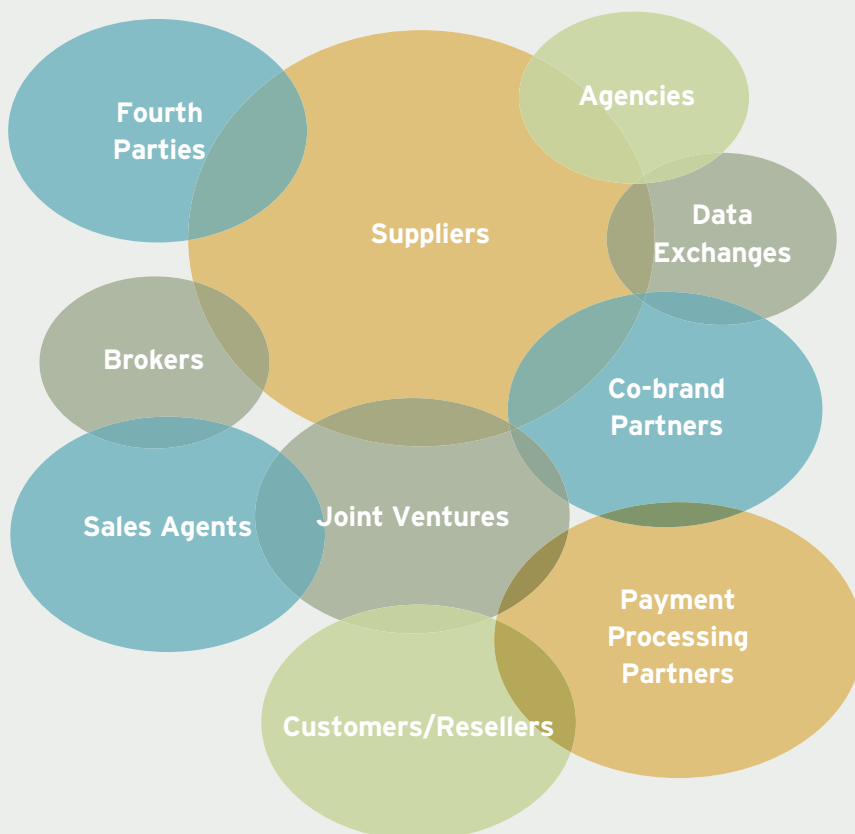
The latest report from TeamMate focuses on techniques audit leaders are using to enhance their risk assessment and audit planning processes.

Read the full report at:
[TeamMateSolutions.com/Enhance](https://www.teammatesolutions.com/enhance)

A smarter approach to third-party risk

Adopting a focused, collaborative strategy can help improve management of outsourced service providers.

**Michael Rose
and Dennis Frio**



For many organizations, third-party risk became a serious topic of conversation in late 2013 when the U.S. Office of the Comptroller of the Currency (OCC) released its 2013-29 bulletin, *Third-party Relationships: Risk Management Guidance*, replacing its more basic principles from 2001. Although some businesses had previously begun addressing third-party data security concerns, most were not evaluating controls across the full spectrum of third-party risks before this new guidance was issued.

The near implosion of the global financial system several years ago played a large part in the increased focus on third-party risk management. It placed a direct light on critical banking operations that had been outsourced to third parties. Financial institutions, starting with national banks, were now being held responsible not only for their own risk management practices but for those

of the third parties they rely on. And of course, these risks extended to industries far beyond financial services. High-profile data breaches at well-known corporations brought additional attention to the role third parties play and the impact they can have on a company's clients and employees.

Today, organizations across industries continue to look for ways to lower costs and increase efficiencies by outsourcing services to third parties. The trend has led companies to expand or optimize their third-party risk programs. Many programs, especially within regulated industries, are evolving to meet business performance goals and regulatory expectations, requiring the right balance between managing risks and stifling the business, without costing too much. Organizations have invested significant capital toward hiring qualified staff, implementing an effective governance and organizational structure, and procuring the right technology to run third-party risk programs.

Resources and skills should center on risks most impactful to the business.

But as these programs have developed, are they truly efficient and sustainable? For many, the answer is no. Organizations are finding they lack risk management efficiencies to adequately support business objectives. Business units find themselves unable to contract with third parties as quickly as they have in the past, delaying the launch of new products and services. The experience has left business leaders frustrated, often pitting procurement and risk management functions at odds over how much risk management overhead is enough.

So what are forward-thinking companies doing? First, they focus with laser precision on the third parties

and services that represent the biggest risks and they efficiently implement strategies to manage them. Second, they realize the value of pooling resources and sharing risk intelligence with their peers. This two-pronged approach yields more robust and efficient management of third-party risk, with internal audit playing a key role in the process.

IDENTIFY THE GREATEST RISKS

Organizations need to develop plans to mitigate and monitor those threats that create the biggest impact on business operations. Resources and skills should center on what matters most to the business, which requires careful planning and a true understanding of the third-party risk profile.

Organizations focused on high-impact risks take a smarter approach by creating risk profiles at the service and third-party levels. They understand the inherent risk of the services they procure and the specific due diligence required to evaluate the third party's control environment. This knowledge limits the need to repeatedly ask questions of the business each time they require services. This approach enables the organization to shift focus to exceptions that don't meet the standard risk profile for the outsourced service. Other attributes of forward-looking companies with a desire to work smarter include:

- » Maintaining an accurate and ongoing inventory of third parties and their services with a map to the specific risks to be assessed and monitored (e.g., those third parties that have access to personally identifiable information for employees or clients).
- » Evaluating and managing preferred suppliers for each expenditure category, eliminating those that don't fit the

Only about **1 in 5** finance executives say they frequently evaluate the security efforts of their suppliers and customers, according to a 2017 CFO Research study.

THE RIGHT BALANCE

Striking an effective balance enables third-party programs to manage risk while supporting business objectives.



organization's defined criteria (including risk profiles).

- » Defining inherent risk rating by service type and managing to those exceptions as described earlier.
- » Communicating third-party risk in business terms using advanced data analytics.
- » Developing key risk and key performance indicators that help identify areas where third-party risk levels may be increasing.
- » Actively monitoring third-party networks for signs of security incidents and malicious activity using threat intelligence feeds such as BitSight, RiskRecon, or SecurityScorecard.
- » Managing reputation and compliance risks, such as negative news and new regulations, with continuous monitoring tools.
- » Understanding and monitoring geopolitical risk for outsourced services.
- » Lowering program costs by implementing integrated third-party risk technology solutions.

Internal audit should help ensure that the business is managing these processes effectively. Moreover, it should make sure the third-party risk management team's program is updated as new

risks are identified and evaluate the overall governance and risk management program each year to determine whether the greatest effort is focused on the highest risks.

OPTIMIZE DUE DILIGENCE

A company's third-party risk programs can raise hundreds of due diligence questions. Targeted areas commonly include information security, business continuity/disaster recovery, legal and compliance, technology systems, and financial, to name just a few. Due diligence is often performed manually across these areas, and the process can be time consuming. Third-party risk leaders first need to understand the outsourced service to determine risk exposure and appetite and then send the right questionnaires to the third party, hoping they're completed and returned on time. Leaders must then review the responses, followed by issuance of risk recommendations—all before the business can sign a contract.

Many organizations seeking a better approach are beginning to value the concept of group intelligence and consortiums as a means of sharing third-party due diligence data. They've discovered that third-party risk is not an area one company should solve on its own. When it comes to critical services, nearly every organization—

regardless of industry—will most likely be sharing a third party with competitors or industry peers. Why should an organization develop its own set of risk domains and due diligence questions when others are compiling the same information?

Third-party companies receive numerous risk questionnaires from their other customers and most likely do not maintain consistency across all their responses. More importantly, when an incident occurs with a third party, it can affect multiple clients. Having the ability to collaborate quickly with industry

who share the same third parties have the opportunity to collaborate over on-site visits and data verification exercises, aimed at lowering costs and improving data consistency. The consortium is designed to adjust over time as the threat landscape changes and improvements are made.

Consortium models are not new and have proven successful in certain circumstances. Many forward-looking companies are now evaluating risk consortiums as they seek broader views on how risks are managed across their own industries, in light of pressure to reduce costs and the need to increase efficiency. Internal audit has an important role with regard to consortiums. Auditors can examine the integrity of the consortium technology, access and security control, permissions, and data integration into company systems. The integrity of the data used by members of the consortium is critical, and it constitutes an area of high risk and priority. Auditors may also want to determine whether the consortium has been reviewed by Legal to ensure the arrangement does not run afoul of anti-trust regulations.

Consortiums are designed to adjust over time as the threat landscape changes.

partners to respond to risk and potential fraud provides a consistent and more efficient way to address the impact.

As an example, four global investment banking and wealth management companies, along with a leading data aggregator, collaborated to build a third-party risk consortium designed to solve the inefficiencies created by their individual third-party risk programs. They developed a centralized data utility that enables firms to standardize and simplify their third-party risk management programs—specifically, due diligence and ongoing monitoring processes. The utility simplifies these processes considerably by aggregating third-party data in a centralized, multi-lateral model. Members can download third-party due diligence responses on demand as opposed to sending out individual questionnaires. They can also receive proactive notification of negative news and relevant events (e.g., mergers/divestitures) as well as monitor information security threats and financial viability measures in one centralized utility. Moreover, members

ADDITIONAL AREAS OF FOCUS FOR INTERNAL AUDIT

Because third-party risk can affect the whole business, internal audit is in a unique position to assist by performing monitoring activities and reporting on its organizationwide findings. As the third line of defense, internal audit provides assurance on the effectiveness of governance, risk management, and internal controls. The third-party risk management team is normally organized as part of the second line of defense, with the business forming its first line. To collaborate effectively, internal audit must understand the working relationship between the business and the third-party risk management team. This process starts with understanding the organization's risk

A recent Thomson Reuters survey shows that **72%** of companies perform initial **third-party** due diligence, but only 36 percent monitor for risk profile changes once third parties are in place.

culture, typically defined as the beliefs, values, attitudes, and behaviors related to risk awareness, risk taking, and risk management. How are the business and third-party risk teams interacting? Do they meet regularly to assess their most critical third parties? Do they agree on the priority of third-party risk?

Internal auditors should examine meeting minutes and other communications between key business leaders and the third-party risk team, as they will provide insight as to the strength of processes and controls around third-party risk. Some additional leading risk management practices for internal audit include:

- » Naming a central point of contact within the audit function to liaise with the third-party risk management team, similar to other enterprise risk functions.
- » If operating in a regulated environment, understanding the guidelines organizational business and risk leaders must follow in addition to any available exam procedures (e.g., OCC's 2017-7, Third-party Relationships: Supplemental Examination Procedures).
- » Determining whether the third-party risk program is focusing its efforts on areas that pose the greatest risk. If so, is the risk management team consistent with this approach? Has it outlined the methodology used to segment risk profiles by severity? Is the team working smart or just working hard?
- » Reviewing the program governance and risk escalation process. Is it disciplined? Is the vendor due diligence robust? Does it include a sufficient approval process?
- » Evaluating the process for handling unplanned terminations for a critical third party. Has

the program adequately defined a workaround while the service is either brought in house or replaced by another third party?

- » Determining what documentation is maintained and whether it provides an adequate audit trail to easily determine what risks and related controls are operating as designed.

KEEPING RISK IN CHECK


Without a doubt, companies need to enhance their third-party risk programs as third parties continue to drive the execution of organizational processes and help optimize performance. The value of managing risks associated with outsourcing a critical business service to a third party is shared across the organization, and it represents a vital component of protecting shareholder value. Internal auditors should keep in mind that their role in this process is critical to providing assurance that third-party risk management performs optimally.

Forward-thinking organizations focus their skills and talents on core business processes and look for creative



TO COMMENT
on this article,
EMAIL the
author at michael.rose@theiia.org

Managing outsourcing risks is vital to protecting shareholder value.

ways to outsource noncore processes. Although more and more organizations are moving in this direction, they must still make sure their vendors are providing consistent, efficient services and that risks associated with using third-party vendors are minimized. 

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

DENNIS FRIO, CPA, is a Business Advisory Services managing director at Grant Thornton LLP.



As businesses strive to find opportunities in a world driven by technological transformation, internal auditors need to continually innovate to stay ahead of the game, says SHANNON URBAN, 2017-2018 chairman of The IIA's North American Board.

The Innovative Internal Auditor

Photographs by Rick Friedman

In today's dynamic and disruptive world, most organizations are undertaking some form of fundamental transformation. Whether they are developing new products and services, refocusing on customer expectations, exploring new technologies, entering the next phase of their push to globalization, or simply seeking new efficiencies, radical change is now an everyday fact of life. Organizations and their internal auditors cannot afford to be static if they want to survive in this environment.

The fact that the rate of change is faster and more intense than ever has major implications for both companies and their internal auditors. It affects the nature of assurance that internal audit stakeholders are seeking, but it can also greatly enhance the speed and quality of the assurance we can provide.

Until recently, assurance was more focused on past events. But the rate of change means that the past is no longer a safe predictor of the future. In today's environment, organizations are calling internal auditors to be more forward-looking. Boards want comfort that as they take their next steps, they can see the potential stumbling blocks and understand what they need to do to get around them.

THE INNOVATIVE INTERNAL AUDITOR

They see internal audit playing a vital role in their efforts to successfully navigate the fast-moving business environment.

That is great news for internal auditors, but it is also a challenge. Traditional auditing is undoubtedly right for many projects; however, when auditors need to deal with the uncertainties inherent in planned business strategies, it is an approach that is less relevant to the velocity of our current business environment. Internal auditors can build upon the steps they have taken to meet these new challenges by focusing more effort on innovation. That is why “Internal Audit Innovation” is my theme as chairman of the North American Board for 2017–2018.

I passionately believe that internal audit has a vital role to play in the success of our organizations. But I also believe that to be up to the task, we need to refresh our commitment to innovation in internal audit. We need to push further and harder on the steps we have taken so far in areas such as audit automation, data analytics, and rethinking our audit processes and methodologies, as well as taking the first steps toward the use of robotics in our audit work. Innovation must be at the core of internal audit’s remit if it is to keep pace with the developments in our own organizations and beyond.

A WORK IN PROGRESS

Many internal auditors are working their hardest to meet their stakeholders’ expectations with often constrained resources—including tight budgets, limited staff, and ever-changing competency demands. Even so, stakeholders seem to continually want internal audit to add more value. Most chief audit executives (CAEs) I meet really care about this issue. They speak with their various stakeholders, try to understand what they value, and modify their audit plans and strategies accordingly. But priorities change much more quickly than in the past, so it can be difficult to see how it is possible to keep doing more and still provide the baseline assurances stakeholders expect.

This is precisely why the innovation mindset is so relevant today. It says internal audit should be a work in progress. That processes are adaptable and open to rapid revision as circumstances change. That audit finds more forward-looking ways of working to adapt to stakeholders’ changing needs. And that technology is a great enabler when fully embraced.

Many internal auditors have already embarked on this journey. But I am calling on everyone to turbocharge their innovation efforts. We can do an even better job of keeping ahead of the rapid developments both within our organizations and beyond if we make a conscious effort to embed innovation in our audit functions.

I urge CAEs and everyone on the internal audit team to make a commitment to embrace innovation today.



Innovation must be at the core of internal audit’s remit if it is to keep pace with the developments in our own organizations and beyond.





The innovation mindset says internal audit should be a work in progress – that processes are adaptable and open to rapid revision.

As I assume the chairmanship of the North American Board, I am extremely grateful and humbled by this opportunity. My career has given me the chance to work with and learn from some incredible internal auditors, and I hope to continue to do that through this role. I would like to thank my employer, EY, for giving me the support and flexibility over the last several years to pursue my interest in IIA leadership opportunities, and for providing me tremendous opportunities to work with some of the leading thinkers on internal audit, risk, and controls. I am also deeply grateful to my husband Matt and sons Luke and Drew for their understanding and support as I pursue my career goals.

In addition to working toward our strategic goals for North America – focused on driving professionalism, advocacy, sustainable value, and The IIA as leader – I am also focused on two objectives that are personally exciting for me. First, I look forward to encouraging all practitioners to become more innovative in how we practice as internal auditors and to adopt a continuous improvement mindset. Second, I will be supporting our diversity and inclusion efforts to both promote success of women in the field of internal auditing and encourage more diversity in our volunteer organization and leadership structure.

OVERCOMING OBSTACLES

Innovating internal audit can be great fun, and those who have done so successfully have reaped the rewards of enhanced risk coverage, deeper insight, and increased stakeholder satisfaction. They have made their organizations nimbler and less prone to surprises. They have often earned a seat at the top table where they provide objective advice and assurance where it is most needed.

But kick-starting an innovative audit culture can be difficult. Because most audit departments work with tight resources, they have little spare time, money, or people power. Working through a packed audit schedule, they may feel that they cannot devote the necessary time and energy to be strategic and innovate.

There is no easy answer to this dilemma. But I urge CAEs and everyone on the internal audit team to make a commitment to embrace innovation today. By making time for regular, meaningful conversations and creative thinking with each other, the rewards will come. Some auditors in a team may take a bit of persuasion that the effort is worthwhile. Some clients may have become comfortable with being audited in a traditional way. And in those cases, auditors will need to have the courage to drive change and insert themselves where they feel they can add value. It takes courage to innovate and to overcome old attitudes resistant to change, to think and act differently, and to show leadership and be an executive in the organization. But by becoming a catalyst for innovation in internal audit, auditors can become a catalyst for change in the organization at large.

THE KEY TO INNOVATION

Even if the audit team is relatively small and cannot create a dedicated innovation center, the CAE can foster a culture of innovation in his or her team. After all, not all innovation aims to reinvent the world.

If I were starting on this journey today, I would sit down with my team and have an open conversation about what the difficult things in internal audit are—the things we spend the most time on. Where could we be more efficient? What are we not covering as well as we'd like? What is hard to do right now to meet the expectations of our stakeholders and to fulfill our mandate? The key to innovation is to turn the answers to these questions into actions.

Heads of audit also could reach out to other innovation hubs within the business and ask for help. Companies are innovating just to survive, so many organizations have developed techniques for driving innovation that audit could learn from. Give someone in your audit function a part-time responsibility to help the innovation

process. And tap into that wealth of often unexploited talent — new professionals. Newer internal audit professionals who aren't tied to tried-and-true ways of working can bring a fresh perspective and an openness to technology as an enabler of innovation.

FROM ANALYTICS TO ROBOTICS

Analytics have been around for a long time. But it is a nut most auditors have not fully cracked, or fully embraced, across the entire audit life cycle. It represents a great opportunity for innovation. Leveraging different types of analytical methods for risk assessment, planning, execution, and reporting can massively boost the efficiency and outcomes of our audit work. Auditors who have not

INNOVATION ACTION POINTS

Have the courage to think and act differently and challenge the status quo.

Commit to change and to an ongoing journey of discovery.

yet innovated their processes in this area can make giant strides very quickly and, in doing so, improve the speed and depth of the assurance they provide.

The biggest conversation I am having in my firm and with cutting-edge internal audit functions is about robotics and what that means for our businesses. Robots, or bots, have moved from the factory floor to finance functions, shared service areas, and other professional areas of work. Internal auditors who take the time to find out what robotics means from a risk and control perspective are likely to be in for a pleasant surprise.

For example, some audit functions are investigating using bots for routine control testing work. They have found that bots can perform those tasks in a fraction of the time and for a fraction of the cost of a real person. So, while some consultants talk about robotics in terms of cutting head count and costs — auditors are beginning to explore how it can alleviate the perennial constraints of resources and budget.

THE 2017-18 IIA NORTH AMERICAN BOARD CHAIRMAN

Shannon Urban is executive director, Risk Advisory, at EY in Boston. With EY since 2001, Urban currently leads growth strategies at the firm as its Northeast Region Internal Audit and Internal Controls Competency leader. She has worked with internal audit departments of all sizes and in multiple industries, including financial services, health care, government, industrial products, and consumer products.

Urban has worked widely on innovation in internal audit, including on EY's internal audit delivery methodology and tools to support internal audit engagements. Previously, she was audit manager at Fidelity Investments, and senior audit officer at State Street Corp., both in Boston, and senior staff auditor at Citizens Financial Group in Providence, R.I.

Urban has been The IIA's North American Board senior vice chair, a Global Board member, an Audit Committee member (2014-2015), and an Institute Relations Committee member (2011-2015). She has been active in The IIA's Greater Boston Chapter as president (2002-2003), treasurer (2001), and a member of its Board of Governors.

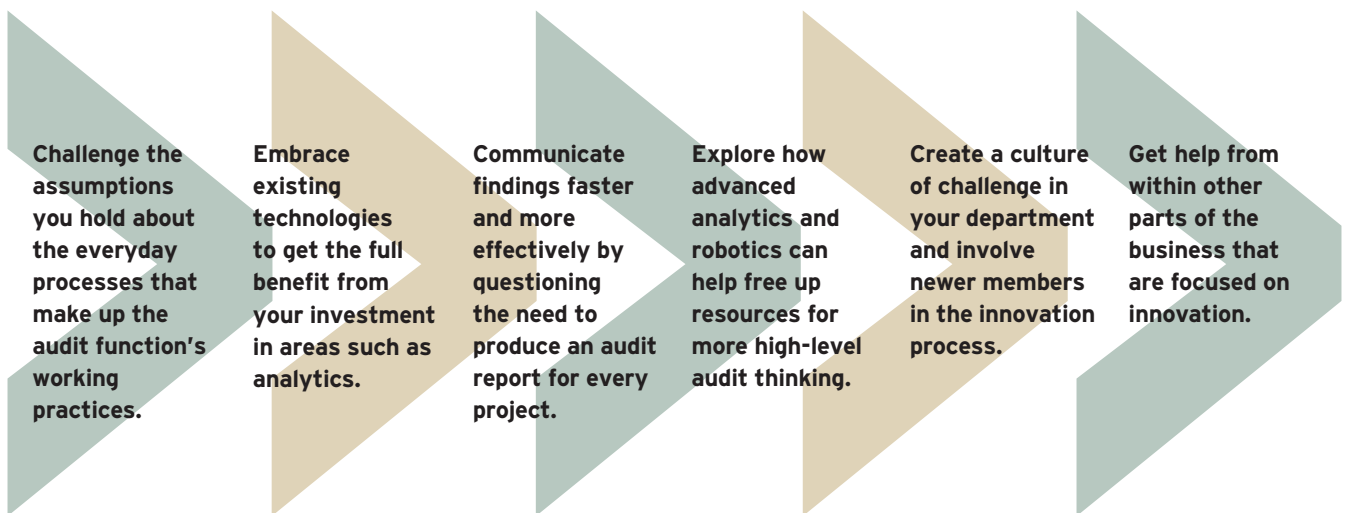


Imagine if the internal audit team could build a series of bots to do all its routine control testing, how much time and how many resources that could free up to focus on higher brain-power auditing and advisory work. It could mean liberating resources to deliver those value-added projects stakeholders demand without sacrificing audit's ability to provide assurance in traditional areas. I see this emerging innovative technology as an internal audit multiplier.

LOOKING CLOSE AT HAND

One of the most powerful tools for innovation in internal audit is fresh thinking. I am very encouraged by how many CAEs with whom I work are open and receptive to new ideas. They want to incorporate those ideas into their work,

But not all innovation relies on technology. For example, not every risk needs a full audit or full audit report. I have worked with many clients to adapt their audit response to the risk, and to be flexible in how they define an audit. For example, they can carry out more remote monitoring, or they can do a design assessment of controls, rather than conduct a full audit. Sometimes, the equivalent of kicking the tires is enough. As we all know, getting an audit report finalized can take a long time because so much value is placed on that report. Yet The IIA's *International Standards for the Professional Practice of Internal Auditing* only requires us to communicate the results of our activities—and that can take various forms. Yes, sometimes a formal audit report is vital. But other forms of communication can be more



but with a busy work schedule, we all know how difficult it can be to turn ideas into action.

Fortunately, innovation can start from looking differently at those things that are closest at hand. When I was thinking about my theme, I realized that the way most internal auditors work has not fundamentally changed over the nearly 25 years I have been in the profession. Of course, the red pencils, hard copy ledgers, and ring binders are gone. We work on computers and smartphones. But most of us could not genuinely say that we are digital internal auditors, even though most of us live and work in a digital world.

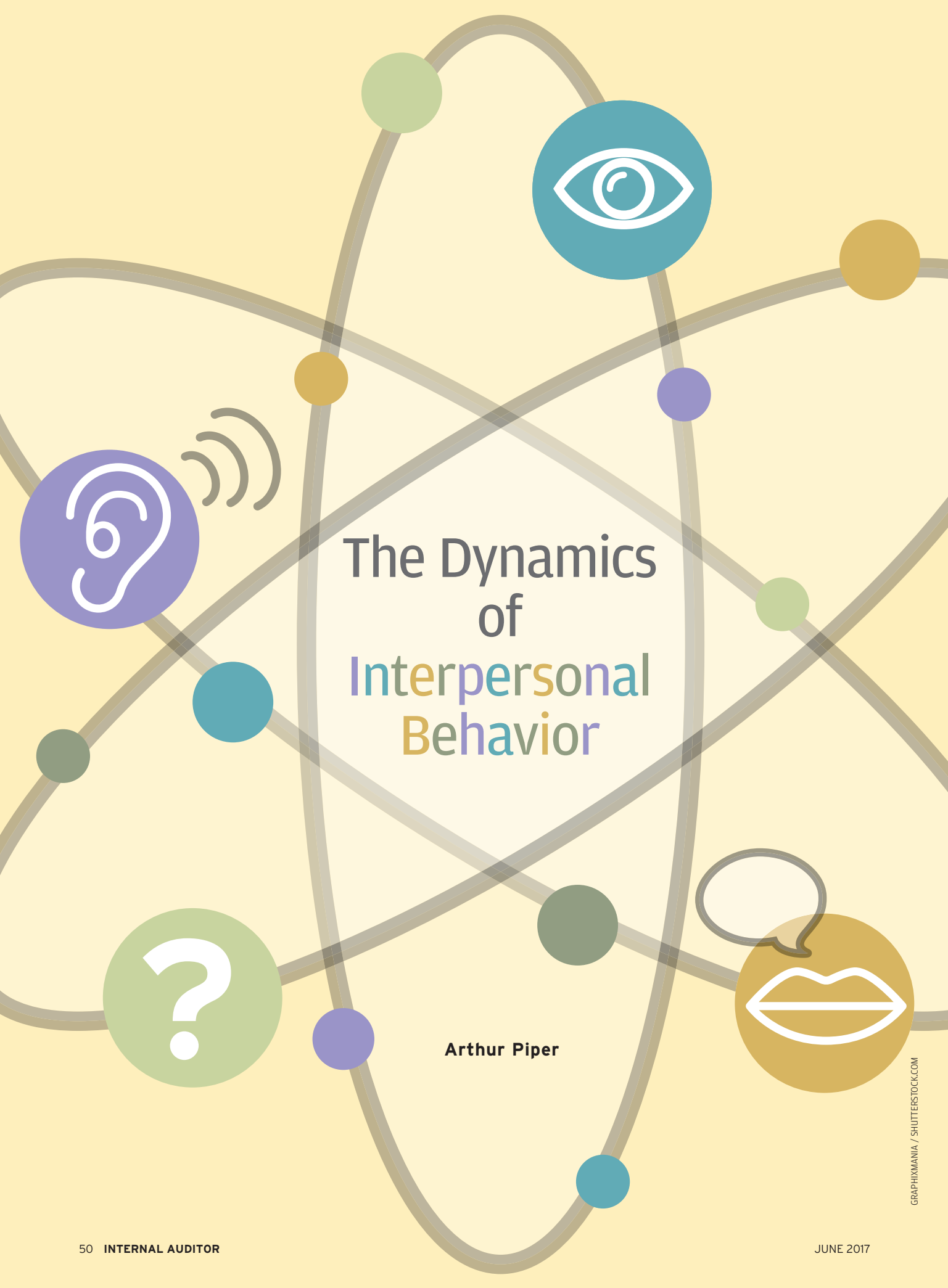
Internal auditors have embraced technology to assist in achieving consistency and quality in our work. But we can go further and fully embrace technology the way our businesses are embracing it. That can be as simple as leveraging the tools that auditors use in their everyday work to their utmost capacity.

effective, including, for example, issuing an executive memo, preparing and delivering a presentation, or providing additional training to deal with control weaknesses. These techniques can be more efficient and timely than an audit report that arrives three to six months after completing the work.

THE ONLY OPTION

Innovation in internal auditing is both crucial for its growth and necessary in meeting the ever-changing needs of stakeholders. It is a messy, frustrating, and ongoing program that demands commitment and courage. And it is fun, surprising, and rewarding. All auditors can take a few easy steps to start, or reboot, their journey today. If we want to understand our stakeholders and serve them well in the future, embracing innovation is the only option. [la](#)

SHANNON URBAN, CIA, CRMA, is an executive director with EY in Boston.



The Dynamics of Interpersonal Behavior

Arthur Piper



To be successful, auditors need to cultivate their soft skills just as much as their technical abilities.

Often described as a soft skill, building strong interpersonal relationships between internal auditors and their wide variety of stakeholders is vital for a function's success. Audit work entails listening, understanding, questioning, explaining, and, sometimes, dealing with sensitive information or challenging people's cherished beliefs. Yet, internal auditors seem to focus their training and continuing education on developing and improving an array of formidable technical skills, seldom paying the same level of attention to sharpening their relationship skills.

Many auditors seem to expect verbal and written communication techniques, active listening and body language traits, and conflict-resolution skills to develop of their own accord—an approach they would never take in building their technical auditing abilities. This occurs even though effectively gathering information from a wide array of sources is germane to the role, and communicating audit findings forms part of the function's requirements under The IIA's *International Standards for the Professional Practice of Internal Auditing*. An audit department that fails to listen and communicate is unlikely to best serve the needs of its stakeholders.

One symptom of a lack of rapport can be seen where audit functions fail to deliver their findings in ways that stakeholders find useful. That suggests and entrenches a lack of understanding about the role of audit and what it can deliver. Agile departments tend to be more in tune with management and the board. They adopt a range of communication formats that better suit the needs of stakeholders, especially in areas such as strategy and emerging risk, where full-blown audit reports may not be as timely or relevant.

SOFT IS HARD

When it comes to understanding the full range of people skills that need to be developed, part of the challenge for anyone in business—not just auditors—is that the terminology is not widely agreed to, says Manny Rosenfeld, senior vice president of internal audit at MoneyGram International in Dallas. Soft skills can be hard to define precisely, but are usually taken to include verbal and written communications, presentation skills, conflict-management skills, leadership, team building, and an ability to assess corporate culture.

In addition to being critical business skills, the ability to form and maintain effective interpersonal relationships

is a life skill that some people seem naturally better at than others, says Rosenfeld, who co-authored *People-Centric Skills: Interpersonal and Communication Skills for Auditors and Business Professionals* (Wiley). “Technical skills are easy to teach, but if you are really interested in developing good people-centric skills, it can take a lifetime to master,” he says.

That is no reason for complacency. While Rosenfeld is skeptical that everyone can be taught full proficiency in certain areas of interpersonal relationships—such as effectively managing teams—all auditors should seek to make progress in the basics. He says there is tremendous potential for developing these skills over time, especially for somebody motivated to succeed. He prefers to talk about interpersonal relationships, because auditors can too often focus on higher-level soft skills—such as report writing and making presentations—while overlooking some of the more fundamental aspects of dealing effectively with people.

“Building trust is absolutely essential in creating successful interpersonal relationships,” Rosenfeld says. “Most people can cultivate trust over time, but auditors need to do it in a few days if they are to conduct a suitable audit.”

This lack of time makes it imperative that auditors become consciously aware that they are trying to build trust. Keeping promises on deadlines, actively listening to feedback, and delivering on audit’s stated goals all help. Trust can be further augmented by showing respect for the opinions of others, he says. That can be difficult because the culture of the audit team or the business may not always be one of openness and mutual respect. He says auditors need to have an open mind and assume that management is trying to do a good job and that differences of opinion between auditor and client can arise simply because they are approaching the same facts from different perspectives.



“Building trust is absolutely essential in creating successful interpersonal relationships.”

Manny Rosenfeld

The most junior auditors need to start learning these techniques from day one. “These skills often receive little attention until auditors become managers,” Rosenfeld says. “But chief audit executives [CAEs] should turbocharge learning for the team in this area because it’s not something people can learn overnight and it is crucial to success.”

IT’S ALL ABOUT STRATEGY

Jim Pelletier, The IIA’s vice president of Professional and Stakeholder Relations, agrees that building effective relationships with audit clients in the business should not be left to chance. “While auditors will have a strategy that will look at how we will use our expertise to deliver an effective audit, we don’t often plan our communications in the same way,” he says. “Why not?”

The group dynamics at work during an audit make this type of planning crucial. Management often views the audit team as a group of outsiders coming to find fault and criticize its work. That can make them overly defensive. In dealing with the arrival of this “outside group” of auditors, the inside group in the business will tend to exaggerate the differences between themselves and the auditors.

“It’s like the situation among sports fans,” Pelletier explains. “In our minds, we ‘dehumanize’ the other team, the players, and their fans, which allows us to rationalize using negative stereotypes, name calling, and insults.” While this is often playful among competing fans, Pelletier says, it can manifest in uglier ways in the office. By negatively labeling auditors as snitches or worse, individuals can then more easily rationalize treating auditors differently. “Many auditors have been lied to or purposefully given misleading or incomplete information,” he says. “This is not acceptable human behavior, but the rationalization brought out by the dynamics between in-groups and out-groups makes it feel okay.”



“We have to acknowledge that whatever people may say to the contrary, being audited feels personal to the client.”

Jim Pelletier

62% of 2,392 human resource executives say **soft skills** are **very** important to hiring candidates in 2017, according to CareerBuilder's Annual Job Forecast.

By labeling auditors as police, for example, the inside group is creating a distance that protects them from personal harm. Pelletier cites psychologist Thomas Szasz, who said: "Every act of conscious learning requires the willingness to suffer an injury to one's self-esteem. That is why young children, before they are aware of their self-importance, learn so quickly."

If this is correct, then auditors represent a threat to a client's self esteem. Pelletier argues that to overcome this obstacle, auditors need to put empathy at the center of their communications strategy. "We have to acknowledge that whatever people may say to the contrary, being audited feels personal to the client," he says. "Instead of being in denial about this, we must recognize that is a natural, negative psychological reaction that derives from the very nature of our role."

Displaying empathy entails making sure you can see things from the perspective of those on the receiving end of the audit—and demonstrate that you care and are truly there to help. "Making the audit feel more like a partnership will help diffuse negative situations," Pelletier says. "Those will still arise, but instead of reaching for the hammer every time, we should try the handshake."

TEAM INTERACTION IS KEY

Wendy Bedwell, assistant professor of psychology at the University of South Florida in Tampa, says good interpersonal skills are at the heart of creating effective audit teams. How well a team cooperates, handles conflict, and solves problems are all predicated on how well team members interact with one another, she says.

Bedwell says people who perform well generally actively listen to others, have good nonverbal skills—such as using the right body language in different situations—and develop an ability to be assertive without coming across as pushy

or aggressive. While she says that how a person tends to interact with others is partially a character trait, she also says it is a skill that any auditor can develop.

It is an area in which CAEs can play a key role. The first step is to measure the interpersonal skills of each auditor. "There are several ways CAEs can measure interpersonal skills," Bedwell says. "Just asking people how they see themselves and observing them when they are in everyday work situations is a great place to start."

She says it is relatively easy to see who is not as competent a listener or talker on the team, and who has assertiveness issues or exhibits poor body language. With more senior staff members, she advises, observe how they handle conflict and solve problems that arise within the team.

"When observing staff members interacting, leaders absolutely cannot interrupt what is going on," she says. "It's natural to want to jump in, give advice, or sort out problems. But it will be much more useful in the long term to diagnose the issues and create a training program to address shortcomings."

The CAE must create the right environment for positive change. "You are setting up expectations and creating a discussion on how to improve skills, so it



“There are several ways CAEs can measure interpersonal skills. Just asking people how they see themselves ... is a great place to start.”

Wendy Bedwell

The CAE must create the right environment for positive change.

is important to present it as a new initiative and as something vital to the success of the team," Bedwell says. "You need to be clear that you do not expect everyone to be perfect, but like with any skill, practice can lead to improvements."

While coaching can be effective, she says, people can also learn from their peers. Putting a good and poor communicator together can be useful. If there

are people with excellent interpersonal skills, Bedwell says it may be worth making them champions and providing them with opportunities to demonstrate their skills. Role playing, practice, and feedback on areas of weakness can result in rapid improvement if the environment is supportive. “For this to really work, the CAE must create alignment between the development of interpersonal skills and the evaluation and reward systems in place,” she says. If those are correctly aligned, behaviors will continue to improve. If not, “that’s where most initiatives fail.”

LEARN TO LISTEN

“When CAEs are working to improve the communication skills of their team, they must remember that we don’t all communicate in the same way,” says Sarah Blackburn, vice chair and chair of the risk and assurance committee at NHS Digital in London, and past-president of the Chartered Institute of Internal Auditors. “We have to build something that is receptive and understanding of the way people prefer to contribute.” For example, she says, some people prefer to listen and digest information during a meeting, so the CAE needs to find different mechanisms—email or social media platforms—where team members can make their contributions in a way that suits them best.

She also says the CAE must set the tone and provide a model for the behavior he or she wants to promote by becoming as good at listening and communicating as possible. That involves reaching out to the business to ask for feedback on both his or her personal performance and on how well the team is doing.

“As an audit committee chair, I get a lot of feedback from management on audit work,” she says. Common complaints include auditors not listening, acting like the police, not taking the time to understand the business’ challenges,

and writing reports about the audit process rather than focusing on what is valuable to management.

“A good CAE will take the opportunity to listen to the audit committee chair, management, and the external

While coaching can be effective, people can also learn from their peers.

auditors,” she says. That kind of listening will pay massive dividends to the audit team’s ability to serve stakeholders well and communicate valuable insight to the top team, she adds.

WELCOME FEEDBACK

“A good indicator of the effectiveness of an audit function and its leadership is how good they are at getting feedback on their performance and having mechanisms in place to act on the results,” says Richard Gossage, managing director at the coaching and communications consultancy Copper Bottom Enterprises in Amersham, U.K. “CAEs should have networks of people such as the audit committee chair, the lead partner of the external audit firm, and others, who they recognize as giving accurate and objective feedback and be rotating around that group regularly.” In accordance with the *Standards*, an external quality survey would provide good information on how internal audit’s communication is perceived.

Because the audit report is the function’s judgment on a particular issue communicated to management or the board, feedback on how well the information was gathered and the results communicated should be standard, he says. Quite often, good audit work and analysis can be ruined at the last moment by poorly written reports that fail to convey the relevance of audit findings to the intended audience.



We have to build something that is receptive and understanding of the way people prefer to contribute.”

Sarah Blackburn



CAEs should have networks of people ... who they recognize as giving accurate and objective feedback.”

Richard Gossage



TO COMMENT on this article,
EMAIL the author at arthur.piper@theiia.org

“The fundamental cause of a lot of poor audit reporting is that the audit team can no longer see the forest for the trees,” Gossage says. “The report becomes a justification of the work that’s been done and the knowledge of the auditors, which is the symptom of a failure to understand your audience. Auditors fail to realize that the report is part of the ongoing dialogue with their audience.”

Gossage advises auditors to learn to see their reports as enabling tools for the business—not ends in themselves. That can require a shift in mindset and a willingness to try different types of communication. Being clear about the purpose of each communication and having a firm grasp of stakeholder expectations will make planning and delivering it much more effective, he says.

AN EMPOWERING EXERCISE

Developing sound interpersonal relationships is a difficult but crucial task for internal auditors. It can make the difference between effective and ineffective audits and audit teams. That is not something that should be left to chance—even though it often is. Building trust, demonstrating empathy, listening, seeking feedback within the team and among stakeholders, and acting to improve shortcomings are all important steps along the way. It may not be easy, but, as Gossage says, “it is a surprisingly empowering process.” [Ia](#)

ARTHUR PIPER is a U.K.-based writer who specializes in corporate governance, internal auditing, risk management, and technology.



Engage and Connect Globally

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

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

www.theiia.org/advertise



2015-1635



Audit Management Software

✓ No Gimmicks

✓ No Metaphors

✓ No Ridiculous Claims

✓ No Clichés

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

Just Brilliant Software.

Find out more at www.mkinsight.com

Trusted by Companies, Governments and Individuals Worldwide.

Opportunity from disruption

Adopting six traits can enable internal audit functions to become more agile in the face of change.

Jason Pett
Mark Kristall
Deborah Mack

Disruptions affect us all, whether they are internal, such as new technology implementation, or external such as new business models, new forms of competition, or regulatory changes. These significant, quickly developing, and potentially unanticipated events create risk and opportunity that demand the attention and resources of the business.

Unlike other risks, the speed at which disruptive events can appear and with which the business needs to react, doesn't lend itself to the notion of internal audit having a year or two to identify related risks, understand them, get projects on an audit plan, and conduct the audits. If auditors don't help the business address disruption-related risks as they occur, the business will charge ahead, potentially increasing risk or bypassing opportunity.

Stakeholders view internal audit's involvement in disruptive events as necessary and meaningful, and their expectations of practitioners continue to rise. The more auditors do, the more stakeholders realize what internal audit is capable of doing, and the more stakeholders ask of them. PwC's 2017 State of the Internal Audit Profession study indicates that the vast majority of stakeholders would like internal audit to be more involved: 77 percent of board members and 68 percent of management say the profession's level of involvement in disruption is not sufficient. This presents an opportunity for internal audit to deliver increased value by being involved

early in the process and bringing a risk mindset to the business as it sets its strategy and tactics.

Early and consistent involvement in disruption requires internal audit to get ahead of disruption and be flexible and responsive as it occurs (see “Rethinking Internal Audit” on this page). To do so, the department needs to build certain traits into its DNA to create the agility needed. Agile internal audit functions are those that are adding significant value in areas of disruption by demonstrating six traits.

BE FORWARD THINKING

The key to becoming agile is being more proactive than reactive. That means staying on the forefront of potential business disruption and recognizing that priorities may change quickly during the year—84 percent of agile internal audit functions are mindful of disruption risk and include the possibility as part of audit plan development (vs. 50 percent of less agile survey respondents), according to the State of the Internal Audit Profession study.

Use a Strategic Planning Process

Define how the department will change its processes, technology, and talent to keep pace with the business. This process is more than an administrative “nice to have;” it’s a road map to internal audit’s vision. These changes will take time, budget, and stakeholder buy-in.

Think Differently About Internal Audit’s Risk Assessment Process

Many organizations are doing away with a robust, annual risk assessment interview/survey process and incorporating more frequent processes such as semi-annual or quarterly assessments. Consider whether internal audit interacts enough with key stakeholders throughout the year to keep a more real-time view of likely disruptions and the top risks to the business.

RETHINKING INTERNAL AUDIT

With stakeholder expectations evolving, internal audit leaders need to help their internal audit functions think differently and push beyond standard objectives and deliverables. To paraphrase Albert Einstein, one can’t keep doing the same things over and over again and expect different outcomes. Audit leaders must think more strategically about where they are operating today and what their ideal state would be by asking themselves:

- » Is the internal audit function doing anything different today than it did three years ago?
- » Are those differences marginal or more transformative?
- » Is internal audit realizing value from those changes?
- » Should audit leaders rethink how they are measuring the department’s value?
- » Is transformation and disruption within internal audit required to remain relevant to the business?

One thing that distinguishes internal audit functions that have developed the agility to embrace disruption is that they appear to have a broader view of what is deemed an “auditable risk” than their less agile peers. This is evidenced by their consistent involvement across many disruptors. These functions are twice as likely as their peers to be involved in less traditional, but high-value areas such as helping the organization respond to operational disruption, changes in business strategy, brand and reputation incidents, and digital innovation. They also are far more likely to be involved early in the disruption and strategic business decision-making cycle. They do more to help their organizations proactively manage disruption before processes are fully developed. Moreover, they provide a point of view around disruptive events beyond identifying existing process or control gaps, and they are twice as likely to assist in identifying the potential for a disruptive event to occur.

Reassess Internal Audit’s Risk

Universe This assessment can confirm whether the risk universe captures emerging risk areas and more holistic risk topics that may not yet be embedded within company operations. If the universe is merely capturing everything that exists within the organization today, it is hard to anticipate what disruption-related risks could be coming. These risks, by nature, are ones that may not have an “owner” yet, and therefore are often missed in functionally organized risk universes. One way to mitigate omitting key risks is to formally link the

risk universe to the organization’s strategic goals.

Create Flexibility in the Audit Plan

If there is no room left in the plan after accounting for recurring activities, then it is difficult to find time for more value-added, risk-based projects aligned to disruptive risks. Allocate a percentage of the audit plan to more proactive and strategically aligned audits, of which disruptive events are a part. Also, allocate a portion of the plan to ad-hoc, management requests, or a “buffer” category to gain flexibility during the year as issues arise.

74% of agile internal audit functions **redirect resources** to help their organization manage or respond to disruption, according to PwC's 2017 State of the Internal Audit Profession study.

BE INCLUSIVE

Driving collaboration often falls upon internal audit because of its unique vantage point within the organization. When done well, this responsibility makes it easier for both management and the audit committee to understand the broader risk landscape and delineate between the lines of defense. It also unites the lines of defense in addressing disruption-related risks as they materialize. Given the organization's size, maturity, and industry, the internal audit function may be serving across multiple lines of defense at the same time. But even then, there is an opportunity to promote a common risk universe and risk language by:

- Inventorying all of the organization's various second-line or risk-oriented functions within the first line. Understand what other risk assessments are being performed by those teams and if there is opportunity for alignment.
- Adjusting the frequency and nature of communications between the second-line functions to understand whether any overlap or duplication exists, as well as whether there are opportunities to transition certain risk activities back to the second line.
- Reassessing how the department audits the second line of defense and whether that could impact the "reliance" strategy internal audit places on such functions. Some internal audit functions adopt criteria where partial or full reliance can be considered over certain risks monitored by the second line to free up time for internal audit to focus on high-risk, strategic, or disruptive topics.

BE BUSINESS MINDED

Stakeholders and chief audit executives (CAEs) agree that internal audit functions should comprise future business

leaders. Business acumen positions internal audit functions to help their organizations manage disruption. The question that many organizations struggle with is: Do you hire auditors and teach them the business, or do you hire from the business and teach them how to audit? In either scenario, the ultimate goal is to develop business-minded professionals who operate true to internal audit's mandate and professional standards. Internal audit should:

- Evaluate the training and development balance among general soft skills, internal audit methodology and approaches, IT technical skills, and business acumen. Some internal audit functions have embedded auditors within the business as it is developing new projects and services to bring a risk-and-controls mindset, while concurrently learning more about the business.
- Build business acumen through the recruitment of diverse backgrounds, degrees, and certifications to promote more organic knowledge sharing among the team.

BE FLEXIBLE BY DESIGN

Alternate audit procedures and reporting options allow flexibility in delivering important messages to management and the board without the burden of self-imposed constraints. Methodologies are helpful, but internal auditors need to reflect on whether their actions are focused on risk understanding and reduction or self-imposed protocols. Many internal audit functions are adding

value—particularly in the area of disruptive risks—through assurance and consulting activities such as delving into the likelihood of specific risks to their organization and assessing the organization's readiness to respond to emerging risks. Several use the term *health checks* for these services.

Inventory the Categories of Projects in the Audit Plan Consider the mix of proactive/reactive evaluations,

Alternate audit procedures and reporting options allow flexibility in delivering important messages.

emerging/existing risk focus, short/long durations, and equal/variable coverage. Use the inventory to determine whether the mix embraces a risk-based and value-adding mentality. Some internal audit functions have difficulty breaking the historic cadence of hitting every location or every department in a set time frame, but the objective is managing risk where it is most likely to manifest, not ensuring full coverage.

Evaluate the Nature and Timeliness of Internal Audit's Procedures

Assess whether they are tailored to project needs or predefined protocols. Do all projects have a similar planning and fieldwork duration? Does the department use the same testing techniques across every project? Is there such a long duration between when a project is identified, put on the audit plan, scheduled, performed, and reported that the relative risk has changed by the time it is ultimately reported on, reducing the project's impact? If the audit committee requested an evaluation of a select risk topic by the following week, could



internal audit mobilize, assess, and provide a point of view in time?

Expanding internal audit's procedures can account for variation and support a risk-based, critical-thinking mentality. The PwC study shows that 73 percent of agile internal audit functions change course and evaluate risk at the speed required by the business, compared to 37 percent of less agile survey respondents.

Rethink the Notion of Internal Audit Reports

Some projects simply don't require a full audit report, and others may not warrant a rating. Highly regulated industries have limits to this flexibility, but even in those situations, there is an opportunity to reflect on how protocols are set and whether they are focused on the importance of the message without being overly restrictive or bogged down in wordsmithing.

BE DATA-ENABLED

The more data-centric businesses become, the more data analysis will become a primary internal audit skill. Analytics should be embedded throughout the audit life cycle in risk assessment, audit planning, fieldwork, and reporting to improve internal audit's business insights. How much more is internal audit doing with data now than three years ago? What improvements has it realized? Is internal audit investing in the right resources and training to further advance its capabilities? Consider using data analytics to:

- Help internal audit teams understand traditionally unauditible risk areas, such as those associated with business disruptions, by analyzing trends and correlations that are not evident through process understanding or controls testing—allowing for more direct exception-based analysis.
- Gain deeper insights that increase the value stakeholders perceive

from internal audit projects, such as through expanded coverage, outlier identification, and more targeted root cause analysis.

- Broaden coverage while reducing the need for on-site visits across geographically dispersed locations. This can provide a more comprehensive view of risks and comparable analysis not achieved through a rotational visit model.

BE TALENT READY

Because of the changing risk landscape, keeping pace with the broader capabilities now needed within internal audit is difficult and highly competitive. Some organizations turn to third parties to close internal audit talent gaps, stay contemporary with evolving skill needs, and flex with business change. Others use internal resources to flex

value are using sourcing in more substantive ways than simply accessing its capacity.

CHANGING WITH THE BUSINESS

Internal auditors don't always give themselves enough credit for what they can contribute. At the end of the day, the profession's role is to help identify and mitigate risk for the organization. Given the tumultuous business environment, that mitigation strategy may require more proactive and real-time evaluations of risk. Regardless of whether internal auditors are doing so to deal with disruptive forces or to improve existing activities, creating more agility in their operations is beneficial.

Internal audit remains one of the few departments that is able to take a holistic view across the business. That gives auditors a unique perspective from

The more data-centric businesses become, the more data analysis will become a primary internal audit skill.

with business needs. Is internal audit's current talent model agile? Do audit leaders know where their skills gaps or key dependencies are? Can internal audit respond quickly to a variety of risk needs or management requests, such as those related to business disruption?

- Identify opportunities to create more agility within internal audit's overall talent strategy. Some of these departments employ a core team and leverage personnel from the business or cosource providers to flex up or down at select times or on specific projects.
- Assess whether internal audit is leveraging its cosource providers in the most meaningful ways. Internal audit functions that add

which to provide a point of view around risk management procedures. Perform a self-assessment. How agilely can the internal audit function operate? Where does the department stand in demonstrating the traits necessary to drive value for the business? Identify the steps internal audit plans to take this year, be aggressive with change, and continue to evolve.

JASON PETT, CPA, is U.S. Internal Audit, Compliance, and Risk Management Solutions leader at PwC in Baltimore.

MARK KRISTALL, CPA, CISA, is an Internal Audit, Compliance, and Risk Management Solutions partner at PwC in Boston.

DEBORAH MACK, CIA, CISA, is an Internal Audit, Compliance, and Risk Management Solutions director at PwC in New York.

Governance Perspectives

BY MELISSA RYAN EDITED BY MARK BRINKLEY

NAVIGATING PRIVACY IN A SEA OF CHANGE

New data protection regulations require thoughtful analysis and incorporation into the organization's governance model.

In the global governance landscape—including risk, audit, and compliance functions—change is pervasive and continuous, making oversight and management of change critical to an organization's governance model. There is perhaps no better example than the ongoing upheaval, questions, and transformation occurring in the European Union (EU) in regard to data protection regulations. Following the finalization of the General Data Protection Regulation (GDPR), which goes into effect May 25, 2018, legal challenges and a stream of questions began immediately. While these events may seem removed from daily concern for U.S.-based organizations, the GDPR is required to operate in the EU/European Economic Area and can no longer be a casual function for organizations.

The GDPR focuses on personal data and, specifically, the right to privacy—that is on any information relating

to the data subject, who can be identified, directly or indirectly, by reference to an identification number or to one or more specific factors, such as: name, birth date, gender, address, phone number, resume or talent information, national identifiers, or bank account or credit card numbers. These broad considerations require analysis by compliance and audit professionals to ensure risks are identified and addressed and control points captured.

Both data controllers and data processors have specific obligations under the new regulation. The data controller is the organization that controls access to and processing of personal information; the data controller determines the purposes and means of the processing of personal data. The data processor is the natural or legal person, public authority, agency, or any other body, including service providers, that processes personal data on behalf of the controller.

While core elements of the regulation are based on prior requirements such as fairness, transparency, purpose limitation, data minimization, quality, security, and confidentiality, the new regulation introduces the accountability principle, providing a direct requirement for oversight and governance of the privacy program.

The changes incorporated into the new regulations require focus, analysis, investment, and incorporation of privacy governance into an organization's governance model, including the audit universe and plan. Review and assessment of these structures should be part of the ongoing audit plan.

Extraterritoriality Effect

The GDPR regulations were designed to extend beyond the EU and do not exclude organizations based on size or corporate jurisdiction. Even businesses without a geographical presence in the EU may fall under the scope

READ MORE ON GOVERNANCE visit the “Marks on Governance” blog at InternalAuditor.org/norman-marks



of the regulation. This can be triggered simply by providing goods or services to EU citizens or by allowing individuals to create user online accounts or profiles that can then be tracked and monitored. EU-based organizations must comply with the regulation based on their jurisdiction. Internal audit should coordinate with compliance and privacy professionals to ensure the new requirements are understood and assessed.

Program Governance and Policy Management Organizations must identify the privacy/data protection program owner and name a data privacy officer. This owner must be aligned organizationally to allow for oversight of the many departments required to participate. Given the extensive requirements associated with the GDPR, full compliance cannot be achieved through disparate or disconnected efforts. Further, application of organizationwide policies, procedures, controls, and monitoring will help ensure consistent alignment of data protection requirements across locations and operations. Privacy program reviews should consider applicable policy updates to ensure specific consideration is given to the regulation within the company's privacy policy. In addition, given the cross-functional reach of privacy requirements, auditors should ensure updates are considered within other functional policies such as software development (e.g., privacy by design considerations) and human resources (e.g., employee data management practices).

Data Mapping and Privacy Impact Assessments Understanding the scope and associated obligations is critical in establishing any governance program. The GDPR considers the activities of data mapping—identification and classification of information assets—and a privacy impact assessment. The results of these activities will guide the remaining program structure and assessment activities. Auditors should coordinate with the compliance or privacy team to ensure these key scoping steps are completed. They provide the foundation for the privacy program assessment as well as key inputs into overall audit universe and risk assessment activities, and thus should be incorporated into audit planning and testing programs.

Contract Management Contractual partnerships and organizations also are in scope for considering the impact to privacy, as often these entities touch, handle, or transfer data. Through an established contract management process, an organization can identify, assess, and respond to data protection obligations across entities. Processes should consider both client contracts, which may require use of standard contractual clauses for cross-border transfers, and vendor and supplier contracts. Within vendor and supplier contracts, companies must ensure obligations are extended to the partner organizations. Internal

audit should review contract management procedures with legal and procurement teams to ensure processes are in place to extend and monitor compliance with obligations.

Notice and Consent Obligations Specific obligations for notice and consent may vary based on an organization's service offering and client interactions. The GDPR requires specific, informed, unambiguous, and in some cases explicit consent to process personal data. Audit should review these processes to ensure both internal associate and client data is maintained and used in accordance with the notice and consent structures in place, or that necessary modifications are made.

Operational Considerations Organizations also must consider storage and movement of personal data within their systems, especially if data is being transferred to or accessed from a non-EU country. A "cross-border transfer" considers both actual data movements and access to the data from outside the originating jurisdiction. Collecting, recording, accessing, using, storing, retrieving, or reading data outside the originating jurisdiction constitutes a transfer. Auditors should incorporate into annual test plans both access-based and process-based control tests to ensure data transfers are managed correctly.

Data Security Considerations While obligations for appropriate technical and organizational measures continue to apply as established by prior regulations, the GDPR includes enhanced breach notification obligations. As such, organizations must ensure their incident response policies and procedures align with the requirements. Review of both incident response and overall security controls should be included in audit's annual plan to ensure a timely response is possible and, if not, that adjustments are made.

These steps can set a course toward governance structures aligned with the data protection regulations. Repercussions of noncompliance are high, with impact to core operations and fines potentially reaching 2 percent to 4 percent of global revenues. Internal audit is key in enhancing ongoing compliance.

As the global privacy landscape changes, organizations must establish both privacy governance structures and a regulatory change management process. This includes defining ownership, refining assessments to incorporate new and changed requirements, and continuing to enhance internal plans and programs. Change must be part of the governance model for privacy and data protection, and auditors should review these structures to confirm appropriateness. [la](#)

MELISSA RYAN, CRMA, is a practice director at Asureti in Lenexa, Kan.



BY J. MICHAEL JACKA

NO MORE EXCUSES

To move the profession forward, internal auditors must overcome their resistance to change.

Recent surveys show a continuing gap between what executive management and board members expect, and what internal audit delivers. Audit professionals insist they want to close that gap. So, why isn't it happening?

People are not comfortable with change, often hiding their resistance under a veneer of excuses. If it weren't for one reason or another, they say, they could change. Internal audit is no different. Several excuses, from specific to more general, are evidence of a department that may not be willing to accept the risk of—and need for—change.

It takes too long to issue audit reports with corrective action. Sorry, no matter what you think, the audit is not complete until the client agrees on corrective action. You can say you issued the report, you can say you hit your milestones, and you can say the department is successful because departmental metrics are being met—but until agreement is reached with the client, nothing has happened. Find out why you have trouble

establishing that agreement, find the root cause of the problem, and then solve it. Be an auditor.


We report to the audit committee; we don't need to report administratively to the CEO. Reasons for this one abound. For example, the CEO doesn't have time, internal audit has a better relationship with a different member of the C-suite, or the current relationship has no impact on the department's effectiveness. Unfortunately, without direct communication with the CEO, internal audit does not have access to the strategic information necessary to accomplish its objectives, is not considered an equal with others in executive management, and is fooling itself if it thinks it can become a trusted advisor.

We don't have time for [blank]. Fill in the blank with just about anything. We don't have time for training, for nonfinancial audits, for special requests, for anything out of the ordinary. To prove there is always time for something important, try reducing your audit schedule by one audit—just one audit. First,

you may notice no one really misses it. More importantly, notice you now have time to accomplish that project you didn't have time for.

You don't understand, we just can't do that. Try explaining what it is we don't understand. In the process, you will realize that you are just making excuses. You can, indeed, do it. You just have to get past the fears—fear of your superiors, fear of lost security, and the fear of trying something new.

The primary impediment to progress is resistance to change. And internal auditors must recognize that their excuses are nothing more than a subterfuge that allows change avoidance. Just as internal audit refuses to accept clients' excuses, it must recognize and eliminate the excuses that keep the department from moving forward.

What excuses are you making that keep you from effecting real change? 

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

Eye on Business

SPEAKING OUT

Courage is a prerequisite for a job that requires reporting executive misconduct.



GREG GROCHOLSKI
Vice President, CAE
SABIC



DAN WILLIAMS
Senior Vice President,
Internal Audit
Darden Restaurants

What challenges do internal auditors face when speaking out about fraud or misconduct at the executive level?

WILLIAMS One of the hurdles internal audit may face is gaining an appropriate level of support from senior management or the audit committee. Due to established relationships and common reporting structures, it may sometimes be easier for senior management or the audit committee to side with the executive. One tactic senior management might use is to avoid denial of the facts, focusing instead on helping the executive minimize the incident by painting the matter as “gray” rather than “black and white.”

GROCHOLSKI Let’s assume the fraud or misconduct has been investigated by the chief audit executive (CAE) and proven. The first challenge would be the CAE’s lack of experience in dealing with these tough matters. Let’s face it, we hope not to have a

lot of experience in this area. But should it happen, the CAE needs to dig deep and develop a plan to determine who needs to be involved, who needs to know about it, how to pursue it, and when—not whether—to inform the audit committee. Have courage: These matters can involve the highest and largest personas in the company. Be thorough: One sign of incompleteness may water down the entire issue. Anticipate reactions: Clearly communicate to the executive’s superiors—and/or the audit committee—the results of your investigation and anticipate how they may react.

How can internal auditors find courage, despite these challenges?

GROCHOLSKI First, “finding courage” should have been considered before taking the CAE role. Courage is a fundamental requirement of the job. The audit committee can help immensely in supporting the CAE through

the matter. At the end of the day, the CAE’s reputation, too, is on the line in terms of how well he or she maintained confidentiality, avoided character assassination, and professionally managed the matter. Depending on the issue, CAEs need to think through the legal implications—such as potential crimes and required disclosures—and this will sometimes force courage on the CAE.

WILLIAMS Auditors should realize that doing the right thing is not always easy. They are frequently put in positions where they must exhibit courageous behavior, and they should be ready to demonstrate unwavering commitment to an ethical environment. The audit profession is founded on ethical standards, and there are resources auditors can reference as they fulfill their responsibilities. They can leverage the company’s code of business conduct, code of ethics, internal audit and

READ MORE ON TODAY’S BUSINESS ISSUES follow @IaMag_IIA on Twitter



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

audit committee charters, and other governance policies, while resources such as The IIA's *International Standards for the Professional Practice of Internal Auditing* offer further support.

What should internal audit do if it encounters resistance when reporting the issue?

WILLIAMS Internal audit should discuss the situation with its direct administrative reporting manager and make its case as to why the executive's actions should be further assessed. This may require special handling, depending on who the executive is and the specifics around the organization's formal/informal reporting structure. If met with resistance, internal audit should explain the significance of the compelling observations gathered and the obligation to elevate the matter if it is not vetted with an appropriate level of attention. Incremental escalation then generally includes separate discussions with other executives—general counsel, the chief financial officer (CFO), the CEO—relevant to aligning on investigative actions and next steps. If internal audit is still not getting support, it should let the executive team know that it has no choice but to discuss the matter directly with the audit committee chair.

GROCHOLSKI CAEs report to the audit committee for a reason—for independence. The CAE needs to investigate the matter and discuss it with the audit committee. Resistance from executive management needs to be vetted during the investigation and raised to the audit committee immediately if it prevents the CAE from doing what needs to be done.

How can CAEs build relationships to ensure they have support when they need it?

GROCHOLSKI Relationships involve trust, and trust is built over time. CAEs need to demonstrate within their engagement with management and the audit committee that they can be trusted. If you are trusted, if you are professional, if you are seen as objective—and not pursuing an agenda—I firmly believe, based on my own experience, you will have the support when needed. Executive management has a stake in this as well, as this will be a time when they, too, need to display courage, demonstrate tone at the top, and walk the talk—not just talk the talk.

WILLIAMS The optimal time to prepare for an incident like executive fraud and misconduct is when you are not in the middle of the incident. Building a relationship with management and the audit committee chair can help ensure internal audit has the support of the organization when it needs it. Get to know them on a professional and personal basis. Strive to lead by example, demonstrating consistent integrity. Let your engagements and your ability to compromise when appropriate demonstrate that you are a business person who wants to drive value and help the organization achieve its goals.

What are some tips for reporting a major incident that involves senior management?

WILLIAMS Internal audit should use a predetermined escalation and response playbook or policy, if one exists. This document should include a communications cadence that can be used depending on the nature of the incident and who is involved. For example, it should consider formal hierarchy, informal hierarchy, long-standing relationships between other executives, and external auditor expectations.

In general, a good first step is for internal audit to discuss the facts with the general counsel and ethics and compliance officer. This will help ensure consideration of attorney–client privilege. If the general counsel is involved, or has a conflict of interest in the matter, then discuss the matter with the CFO, CEO, or similar executive instead and gain alignment on next steps. Communication with other executives early on may also be necessary, but should always be done on a need-to-know basis. Internal audit should also communicate timely with the audit committee chair, bringing him or her up to speed on the facts and circumstances. The general counsel and audit committee chair should help determine whether an external firm should be engaged, and by whom, to maintain the independence of an investigation. Internal audit's interactions with senior management and the audit committee should address communications with the independent auditor to determine the impact of the matter on its audit of the organization's financial statements and related financial reporting controls.

GROCHOLSKI Follow internal investigative protocols first, even if that includes discussing the matter with the executive vice president of legal, IT, or human resources, or the CEO or CFO. Everyone should understand an investigation serves two purposes—each being equally vital: to prove or disprove the matter. Next, determine when to inform the audit committee chair or the entire committee. Conduct nonintrusive data gathering and see what the data is telling you. Pull additional data if necessary to further prove or disprove initial analysis. All along, document what you do in a way that will serve you well should the matter be referred to external forensics or external legal firms to either continue investigating or because the audit committee wants them to validate your work and conclusions.

There are two stages: 1) observing/hearing about it and 2) proving it. Each stage has its challenges. In the first stage, you may need to look at data, emails, expense reports, or contracts to investigate the matter; you may even have to interview employees. A challenge here may be in just accessing the data/people, as you may need legal, IT, or executive management to be aware of the need to do so. Plan ahead, there may be resistance. Be aware that you will be closely watched to see how you work through this maze of politics, sensitivities, and dealing with large personas in the company. [la](#)



The IIA Congratulates the 2016 Certified Internal Auditor® (CIA®)* Award Winners!

William S. Smith Award – Gold
(Highest Scoring Candidate)
Sarah Gray, CIA *Canada*

Kurt Riedener Award – Bronze
(3rd Highest Scoring Candidate)
Maggie Lau, CIA *Canada*

A.J. Hans Spoel Award – Silver
(2nd Highest Scoring Candidate)
Justin Mahe, CIA *USA*

Dr. Glenn E. Sumners Award – Student
(Highest Scoring Student Candidate)
Tianye Zhang, CIA *China*

The IIA also recognizes the Certificate of Excellence (Next 10 Highest Scoring Individuals) and Certificate of Honor (Next 50 Highest Scoring Individuals) recipients:

Certificate of Excellence:*

Michael Aaron Fleischaker, CIA *USA*
Jennifer M. Herron, CIA *USA*
Sianna Koleva, CIA *Netherlands*
Andrew N. McLaughlin, CIA *USA*

Justin M. Moroder, CIA *USA*
Janne Poutanen, CIA *Finland*
Jason D. Schanno, CIA *USA*
Christopher Siron, CIA *USA*

Kirsten Stevens, CIA *USA*
Tan Yan Wen, CIA *Singapore*

Certificate of Honor:*

Ziad Yousef Solaiman Abdelghani, CIA
IIA–United Arab Emirates
Haris Akhtar Aziz, CIA *IIA–Pakistan*
Brian Douglas Boone, CIA *Sacramento, CA*
Simos Boursalian, CIA *IIA–Greece*
Donald E. Carlson, CIA, *CGAP Austin, TX*
Qaisar Choudhary, CIA *IIA–Qatar*
Andrew J.D. Collins, CIA *Great Britain*
Shellie Ruoff Creson, CIA *Birmingham, AL*
Steven Dassing, CIA *Philadelphia, PA*
Frederique Deniger, CIA *Montreal, Canada*
Dieter Dresel, CIA *IIA–Germany*
Charles W. Edson, CIA *Tidewater, VA*
Bradley Erla, CIA *Lansing, MI*
Douglas D. Forster, CIA *Ottawa, Canada*
Sean Alexander Frasier, CIA *Twin Cities, MN*
Sabrina Gülck, CIA *IIA–Germany*
Andrew Joseph Haynie, CIA *Salt Lake City, UT*

Rui He, CIA *IIA–Germany*
Donal Hewitt, CIA *Red River Valley, ND*
Christian Hilgemann, CIA *IIA–Germany*
Mitsutaka Kimura, CIA, *CFSA IIA–Japan*
Lea Koehnken, CIA *New York, NY*
Jonathan Maxwell Kresser, CIA *San Diego, CA*
Kristin Elizabeth LaBella, CIA *Dallas, TX*
Madison Sokkuan Lai, CIA *Las Vegas, NV*
Kailee D. Levesque, CIA *Ocean State, RI*
Rohan V. Mangalore, CIA *IIA–India*
Julius Peralta Mondala, CIA *IIA–Philippines*
Stephan Mörgeli, CIA *IIA–Switzerland*
Launce Moses, CIA *New York, NY*
Christopher Warren Mutz, CIA *Washington, DC*
Carmen Patton-Minder, CIA *Twin Cities, MN*
Michael J. Peters, CIA *Detroit, MI*
Jessie Pieper, CIA *Madison, WI*

Rhea Rasquinha, CIA *Ontario, Canada*
Philip J. Richard, CIA *Greater Boston, MA*
Nicolas Carlos Rois, CIA *Mexico*
Denton Romans, CIA *Mid-Columbia, WA*
Andrew Simonet, CIA *Twin Cities, MN*
Brian Stevens, CIA *Washington, DC*
Nicki Stewart, CIA *Portland, OR*
Brian A. Stone, CIA *IIA–Philippines*
Anne Maria Truijens, CIA *IIA–Netherlands*
Adrine Tumanyan, CIA *IIA–Armenia*
Drew Desmond Turner, CIA *IIA–Australia*
Luc Van Thielen, CIA *IIA–Belgium*
Ravichandran Asirvatham Whitehead,
CIA, *CRMA Barbados*
Christian Woll, CIA, *CRMA IIA–Germany*
Nanxing Xue, CIA *San Gabriel Valley, CA*
Everet Zicarelli, CIA *Philadelphia, PA*

Join with us in congratulating the following individuals for highest achievement on specialty certification exams.

Certification in Control Self-Assessment® (CCSA®)

Daniela Recknagel, CIA, *CCSA IIA–Germany*

Certified Financial Services Auditor® (CFSA®)

Callan Robert Doak, *CFSA San Francisco, CA*

Certified Government Audit Professional® (CGAP®)

Jeffrey Kowalczyk, *CGAP Philadelphia, PA*

Certification in Risk Management Assurance® (CRMA®)

Matthew A. Keeler, *CRMA Atlanta, GA*

The IIA congratulates all 68 award winners. It is their dedication to their profession and understanding of the benefits and importance of certification that has led each to achieve these honors.

*Awards are based on individual performance on the core CIA exam parts 1, 2, and 3. With year-round testing, award recipients must pass each segment of the exam on their first attempt within one year of beginning the testing process.

IIA Calendar



IIA CONFERENCES

www.theiia.org/conferences

JUNE 6-9

Western Regional Conference

The Anaheim Marriott
Anaheim, CA

JULY 23-26

International Conference

International Convention Centre
Sydney, Australia

AUGUST 16-18

Governance, Risk, and Control Conference

Gaylord Texan
Dallas-Ft. Worth

SEPT. 11-12

Environmental, Health & Safety Exchange

Hyatt Regency St. Louis
St. Louis

SEPT. 17-20

Southern Regional Conference

Hilton Austin
Austin, TX

SEPT. 18-19

Financial Services Exchange

Renaissance Downtown Hotel
Washington, D.C.

OCT. 29-NOV. 1

All Star Conference

The Bellagio
Las Vegas

MARCH 12-14, 2018

General Audit Management Conference

The Aria
Las Vegas

IIA TRAINING

www.theiia.org/training

JUNE 5-14

Operational Auditing: Influencing Positive Change

Online

JUNE 5-23

CIA Learning System Comprehensive Instructor-led Course Part 1

Online

JUNE 6-15

Assessing Risk: Ensuring Internal Audit's Value

Online

JUNE 19-22

Various Courses

Las Vegas

JUNE 19-28

Lean Six Sigma Tools for Internal Audit Fieldwork

Online

JUNE 20-29

Enterprise Risk Management: Elements of the Process

Online

JUNE 27-30

Various Courses

Dallas

JULY 10-19

Value-add Business Controls: The Right Way to Manage Risk

Online

JULY 11-13

Beginning Auditor Tools and Techniques

Operational Auditing: Influencing Positive Change

Raleigh-Durham, NC

JULY 11-20

Lean Six Sigma Tools for Internal Audit Planning

Online

JULY 18-21

Various Courses

Orlando, FL

JULY 19-28

Fundamentals of IT Auditing

Online

JULY 26-27

Data Analysis for Internal Auditors

Online

JULY 26-28

CIA Learning System Comprehensive Instructor-led Course Part 3

Lake Mary, FL

JULY 31-AUGUST 25

CIA Learning System Comprehensive Instructor-led Course Part 3

Online

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



BY CHRISTINE HOGAN HAYES

INTERNAL AUDIT AS POLICE

Perhaps it's time to embrace our image as corporate protectors rather than fighting against it.

As internal auditors, we frequently hear our profession labeled as the organization's police. The comment is made in a critical tone, often accompanied by descriptions of internal audit as a "gotcha" function that seeks to identify and highlight obvious issues. Many of us respond by offering examples of how auditors provide value-added services, form partnerships with the business, and provide recommendations that can improve and strengthen the overall control environment. And while citing this information can help educate clients about our wide variety of roles and responsibilities, I have begun to wonder whether disputing their characterization of the profession is truly effective, appropriate, and even accurate.

When confronted with the police comparison, should we seek to understand where this perception comes from? Auditors are trained to ask thoughtful, open-ended questions as part of our standard walk-throughs. Can we implement the same skills in conversations about the nature of our work? A client's

opinion about the profession may stem from an experience he or she had with an audit team in the past. By identifying what could have been executed differently, we can implement strategies in the current audit to help avoid such an experience from recurring. Or perhaps the client's impression is based on internal audit's portrayal in the media. By discussing what is happening at other companies, internal audit can facilitate dialogue about risk areas of concern that ultimately could be leveraged to improve audit planning and execution.

Simply disagreeing with clients' perceptions of internal audit sets an adversarial atmosphere for the engagement. Is it necessary to disagree, or can we acknowledge their perspective? Then, rather than highlighting our consulting projects, special management requests, and continuous monitoring activities, perhaps we could explain the purpose of our work nondefensively.

Maybe audit clients are not that off base when characterizing internal audit as a policing activity. Similar to police who protect the communities they serve, internal

audit aims to protect the organization by performing risk-based audits that cover financial, operational, and regulatory activities. Internal auditors are trained to identify red flags of fraudulent activity that could harm the organization, similar to a police officer who identifies criminal activity that could harm the community. Internal audit develops rapport with business units to build a foundation for strategic discussions, similar to police who forge positive relationships with schools and neighborhoods to strengthen the bonds of the community.

Although the profession has made considerable strides with its image among stakeholders, comparisons between internal audit and the police are still common. But such opinions do not have to be interpreted as negative or invalidating. Instead, they can be embraced and leveraged to facilitate candid discussions about audit objectives and organizational risk. [la](#)

CHRISTINE HOGAN HAYES
is a senior internal audit specialist at Plymouth Rock Management Co. of New Jersey in Red Bank.

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

2017 FINANCIAL SERVICES EXCHANGE

Connect. Collaborate. Evolve.

SEPT. 18–19

Renaissance Downtown Washington / Washington, DC

Experience a Different Type of Conference

As the regulatory environment becomes more complex, the Financial Services Exchange is the event for internal auditors to learn and share leading practices to navigate through the associated risks.

- “Good insight from actual experiences.”
- “Engaging conversation. Very thought provoking.”
- “Excellent and relevant to where we are trying to go.”

Don't miss this unique blend of interactive sessions and educational presentations.



Register by July 24 and save US\$100.
www.theiia.org/FSE



Financial Services
AUDIT CENTER

2017-0921

Deloitte.



Drive insights

Deloitte helps internal audit leaders make an impact that matters. How? By combining advanced analytics with deep subject matter expertise, proprietary labs, and innovative methods to uncover insights. We help internal audit transform into a function that not only delivers assurance, but also advises and anticipates risk.

Unlock the potential of internal audit. See where insights lead.

www.deloitte.com/us/internalaudit