

Ia

INTERNAL AUDITOR

FEBRUARY 2018

A PUBLICATION OF THE IIA

The CAE and CRO: A Risk Management Collaboration

Know Your EQ

Assessing Corporate Governance Practices

Build Your Personal Brand



BOARD MATTERS

CAEs who understand board priorities can build a sound relationship through effective assurance.

Deloitte.



Are you ready for the future of internal audit?

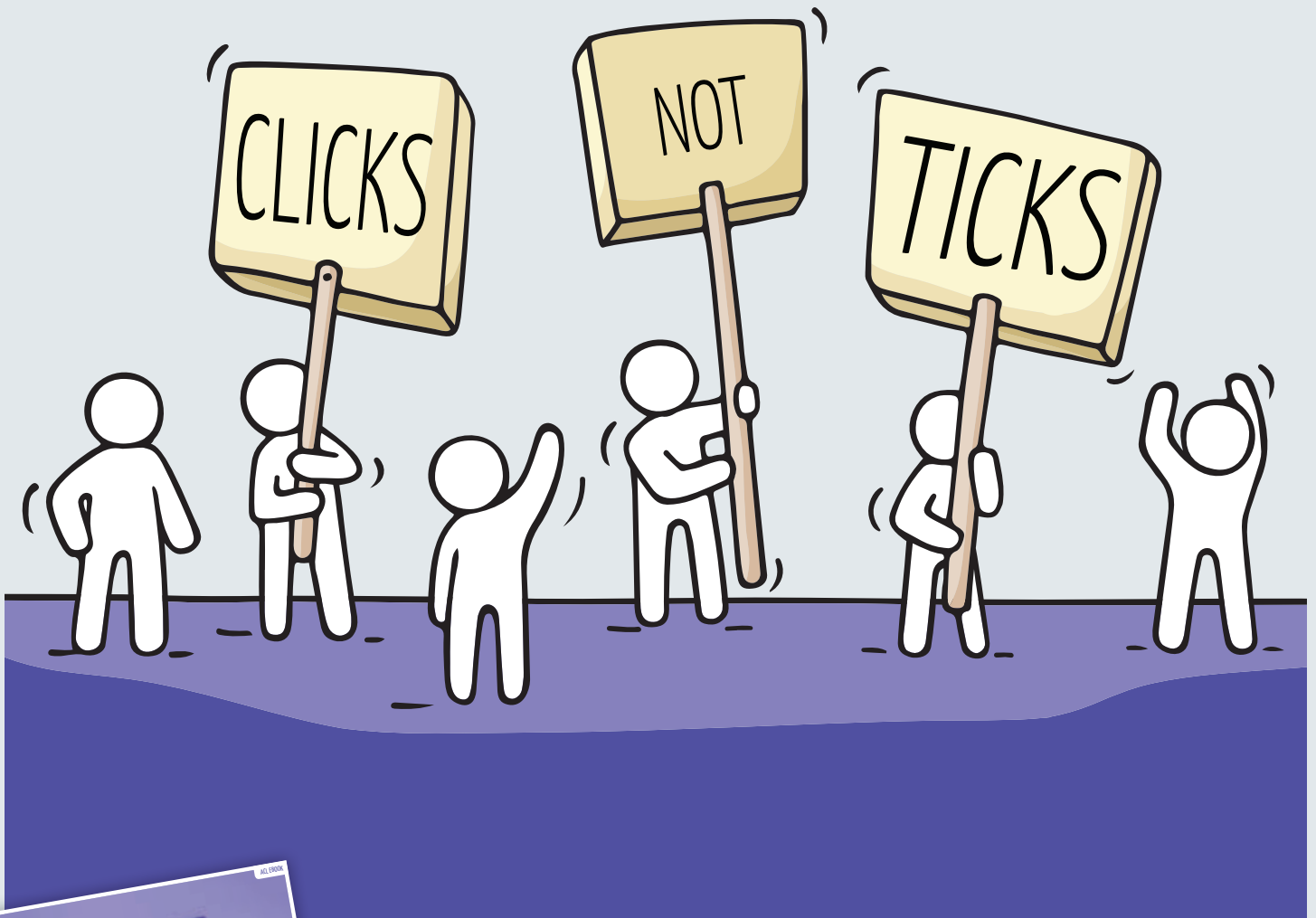
Assure. Advise. Anticipate.

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

www.deloitte.com/us/ia-future

MOVE OVER TICK MARKS

Audit management is better with data automation



Automate data to uncover the risks that matter most in a single lens across your organization
Death of the Tick Mark: How data automation can put an end to manual processes

Download at acl.com/tick-mark »



Meet your challenges when they're still opportunities.

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

rsmus.com

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING



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



FEATURES

24 COVER Board Matters Internal audit and board alignment can best be achieved when each looks to understand the priorities and needs of the other. **BY ARTHUR PIPER**

31 The CAE-CRO Relationship Chief audit executives and chief risk officers can collaborate in many ways to ensure the organization manages risks effectively. **BY CHARLIE WRIGHT**

36 How's Your EQ? Emotional intelligence can help auditors build and maintain positive, productive relationships throughout the organization. **BY J. MICHAEL JACKA**

43 Implementing a Shared Services Model When consolidating services, internal audit's broad knowledge of the business works

to the organization's advantage.

BY DARRICK FULTON AND NANDINI PARCHURE

48 Governance in View Done right, corporate governance audits can generate great value for organizations. **BY DOUG WATT AND BRIAN SCHWARTZ**

54 Your Personal Brand Building a professional identity, and promoting it effectively, can be vital to an internal auditor's career.

BY NANCY HAIG



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

TeamMate+



**Best User
Experience**
in Audit
Management

GRC 20/20



**Best
Product**
in Auditing
Innovations

THE GOLDEN BRIDGE AWARDS

**The biggest prize of all is
our customers' success.**

We're gratified the industry has recognized TeamMate+ as
a major step forward in audit management.

Learn more about the innovations that are getting
TeamMate+ recognized at:

www.TeamMateSolutions.com/Awards

DEPARTMENTS



7 Editor's Note

8 Reader Forum

67 Calendar

PRACTICES

11 Update Innovation and transformation top 2018 list of concerns; scandals lead to tighter controls; and companies look to navigate the GDPR.

14 Back to Basics Successful small audit functions have all the right tools.

16 ITAudit Is CARTA a smarter approach to addressing cybersecurity risks?

19 Risk Watch Blockchain may both produce and help manage risk.

22 Fraud Findings Unscrupulous employees take advantage of a promoter program.

INSIGHTS

60 Governance Perspectives Third-party governance is a must.

63 The Mind of Jacka Are you the type of auditor who sees control issues everywhere you look?

64 Eye on Business CAEs must understand what the audit committee needs.

68 In My Opinion Integrated audits can help improve the organization's operations.

ONLINE InternalAuditor.org



Getting the Word Out

Unless the department markets itself effectively, stakeholders may remain unaware of internal audit's full scope of services.

Profiting From Auctions

Fraud expert Art Stewart discusses measures local governments are taking to prevent fraud in tax deed auctions.

Rising Cyber Risks Affect

Business Plans Most C-suite leaders say their organization has changed business plans or strategies in response to cyberthreats.

Emotional Intelligence

for Auditors Watch a video series with "How's Your EQ?" author Mike Jacka on the value of emotional agility in the workplace.



Customize Your Membership with a Specialty Audit Center

INFLUENTIAL. IMPACTFUL. INDISPENSABLE.



The IIA's Specialty Audit Centers provide targeted resources focused on issues that matter most to you and your stakeholders — to keep you influential, impactful, and indispensable.

Learn more at www.theiia.org/SpecialtyCenters



**The Institute of
Internal Auditors**

-
- GOVERNMENT
 - FINANCIAL SERVICES
 - ENVIRONMENTAL, HEALTH & SAFETY



EQ AND STRESS MANAGEMENT

The holidays put me behind at work. I took some time off, and now that I'm back, I've got a magazine to get out, performance reviews to conduct, presentations to prepare, etc. It's challenging to focus on any one task, making it difficult to complete anything. I can feel my stress level rising.

In this issue's "How's Your EQ?" (page 36) author Mike Jacka considers how internal auditors can use their emotional intelligence (or quotient) (EQ) to build better relationships throughout the organization. But a recent article in the *Harvard Business Review* says we can also use EQ—particularly, self-awareness and self-management—to reduce our stress and help us focus.

According to the author, Kandi Wiens, "one of the reasons why some people get burned out and others don't is because they use their [EQ] to manage their stress." In "Break the Cycle of Stress and Distraction by Using Your Emotional Intelligence," Wiens encourages readers to use their self-awareness to notice when they feel stressed and then take several steps to keep focused. One step we can take, she suggests, is limiting our digital access.

The American Psychological Association's (APA's) 2017 Stress in America report says those who check their email, texts, and social media accounts constantly have higher stress levels than those who don't check as frequently. And those who check their work email constantly on their days off have even higher stress levels. According to the APA report, 65 percent of Americans somewhat or strongly agree that periodically "unplugging" is important to their mental health; however, only 28 percent of those respondents actually report doing so.

Other suggestions offered by Wiens for reducing stress include committing to the recommended seven to eight hours of sleep each night, practicing mindfulness and resisting knee-jerk reactions, and paying more attention to others' feelings and needs. "Studies ... show that shifting our focus to others produces physiological effects that calm us and strengthen our resilience," she writes.

Maybe the best advice I've received on lowering stress and staying focused came from my boss: "Live one day at a time." You can't change the past; you can't control the future. Live in the present and take each day as it comes. Here's to a productive, focused, stress-free 2018!



@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.



Face-to-face Auditing

Mark Ledman is spot-on about auditing outside of email. The use of technology has its place and advantages, but hampers the face-to-face interaction that would help an auditor complete the objectives of an audit. An auditor's personal account of what is going on within the organization is stronger than making assumptions through email. Further, Ledman's point about having an eye or ear on site allows the auditor to minimize instances of rehearsed or prepared statements from the organization. You



also minimize any potential issues with delayed responses or documentation in the native or raw form within concerns of tampering. After all, it is harder for an organization to hide information and emotions when personnel see an auditor in person.

FREDRICK LEE comments on Mark Ledman's "Are You Auditing By Email?" ("In My Opinion," December 2017).

Be Accountable

It is truly remarkable the amount of progress that has been made in the profession. I received my CIA designation several years ago (when there were still four parts), but recently took a look at the CIA exam syllabus in its current form. As I was reading through the content, I thought to myself that this is the type of knowledge that anyone practicing internal auditing should understand. At a minimum, all individuals working in internal audit should possess strong knowledge of the *International Standards for the Professional Practice of Internal Auditing*, which can be

demonstrated by obtaining the Internal Audit Practitioner designation.

Personally, I have experienced a great deal of frustration while advocating for conformance to the *Standards*. I have heard arguments saying that the *Standards* are not prescriptive enough, that there is no consequence to non-conformance, and that they represent a "better practice" that a department should work toward while tackling other high-priority items. While false, it is amazing that some of these comments are so pervasive in the profession.

The bottom line is that board members should be held accountable if they choose to staff an internal audit function that does not conform to the *Standards*. Serious questions need to be asked of that board on how they are sure that they are adequately fulfilling their oversight role given they don't have an internal audit function that conforms to the *Standards*. This is especially critical when capital available from investors is at stake.

I'm honestly surprised that these questions have never been asked in

Ia
INTERNAL
AUDITOR

FEBRUARY 2018
VOLUME LXXV:1

EDITOR IN CHIEF

Anne Millage

MANAGING EDITOR

David Salierno

ASSOCIATE MANAGING EDITOR

Tim McCollum

SENIOR EDITOR

Shannon Steffee

ART DIRECTION

Yacinski Design, LLC

PRODUCTION MANAGER

Gretchen Gorfine

CONTRIBUTING EDITORS

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

EDITORIAL ADVISORY BOARD

Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, CGA, FCIS, CFMA
Mark Brinkley, CIA, CFEA, CRMA
Robin Altia Brown
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Wade Cassels, CIA, CCSA, CRMA, CFE
Daniel J. Clemens, CIA
Michael Cox, FIA(INZ), AT
Dominic Daher, JD, LL.M.
Haylee 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, CPCU, 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
Jack Murray, Jr., CBA, CRP
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Bryant Richards, CIA, CRMA
Jeffrey Ridley, CIA, FCIS, FIA
Marshall Romney, PhD, CPA, CFE
James Roth, PhD, 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, CFEA, CRMA
Benito Ybarra, CIA

IIA PRESIDENT AND CEO

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

IIA CHAIRMAN OF THE BOARD

J. Michael Peppers, CIA,
QIAL, CRMA


PUBLISHED BY THE
INSTITUTE OF INTERNAL
AUDITORS INC.

CONTACT INFORMATION

ADVERTISING
advertising@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
InternalAuditor.org (click on "Writer's Guidelines")

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

cases where shareholders have sued a corporation or where regulators have investigated and penalized a corporation. Why doesn't your internal audit function conform to the *Standards*?

KEITH DUFF comments on the *Chambers on the Profession* blog post, "Internal Audit Standards: The Only Option Is to Conform" (*InternalAuditor.org*).

Adaptable Audit Approach

As the CAE of a large organization, my team and I are constantly on the lookout for examples of audit groups that have increased their value proposition by successfully transitioning their audit approach to be more agile and adaptive to organizational and environmental changes. Ruth Prickett's article highlighted many ideas we are considering, but took it a step

further by pointing out how auditor skills also must change to emphasize data, technology, and business skills. Attracting and retaining professionals with the skills we need to provide assurance in the future is a major challenge and one that CAEs must embrace. This is an exciting time to be a practitioner.

DOUG WATT comments on Ruth Prickett's "Agile Performer" (December 2017).

Address the Root Cause

Jim Pelletier's blog post got me thinking about the quality of recommendations, as they are our best tool to add value. The No. 1 reason why recommendations do not result in positive change is their failure to be based on solid root-cause analysis. If they don't address the root cause, how could they target the right

agents of change, the right resources, and the right systems? Well done, and thank you for a very enlightening post.

YVES GENEST comments on the *Points of View by Pelletier* blog post, "5 Tips to Avoid Calling the Plumber" (*InternalAuditor.org*).

Change Is Happening

Thanks for your insight and guidance as we move into the new year. Change seems to be happening at the speed of light. Christmas this year brought new smart TVs, smart phones, and now, smart homes thanks to artificial intelligence (AI) such as Amazon's Echo. Internal audit will need to quickly learn how AI will be used within our companies.

TAMMY GUTHRIE comments on the *Chambers on the Profession* blog post, "Five Internal Audit Resolutions for 2018 and Beyond" (*InternalAuditor.org*).

S | C SECURANCE CONSULTING

OVERCOME YOUR GREATEST RISK.

RISK | SECURITY | COMPLIANCE | PEACE OF MIND
www.SeuranceConsulting.com • 877.578.0215

Connecting the World Through Innovation

Network | Learn | Innovate | Lead

DUBAI, UAE, 6-9 MAY 2018



Join Industry Leaders in Dubai

Register today and take advantage of this amazing opportunity to learn from and network with peers from around the globe. Experience dynamic sessions highlighting solutions to help audit leaders worldwide keep pace with changes in technology and techniques.

100+

Speakers
From Around
the Globe

70+

Sessions in
10 Educational
Streams

2,500+

Audit Industry
Practitioners
& Providers From
100+ Countries



NEW CONFIRMED SPEAKER

Tanmay Bakshi, Neural Network Architect, Honorary IBM Cloud Advisor

Open Source Development: Information Security and Technology Auditing

This 14-year-old phenomenon has taken the technology world by storm. His expertise in neural networks and artificial intelligence is transforming the way technology is used to overcome obstacles in fields like healthcare.

Register Today
ic.globaliia.org

THE INSTITUTE OF INTERNAL AUDITORS
**INTERNATIONAL
CONFERENCE**
DUBAI, UAE / 6-9 MAY 2018



2017-1139

Japan firms roll out controls after scandals... Change tops board priorities... Time running out for GDPR readiness... New PCAOB chair and members.

Update



COMPANY EXECS FOCUS ON DISRUPTION

Rapid technological changes and disruptive innovation rank as the top concerns among board members and CEOs worldwide, a recent study reports. Specifically, leaders are concerned that changes are outpacing the organization's ability to compete or manage associated risks effectively, according to Executive Perspectives on Top Risks, conducted by Protiviti Inc. and North Carolina State University's Enterprise Risk Management Initiative.

Disruption and technological change outranked fears about economic uncertainty and regulatory scrutiny, which had topped the

High-speed innovation and digital transformation top leaders' concerns for 2018.

survey's list of executive and board risk issues over the past several years. In a separate report from EY, both institutional investors and business leaders say new technology innovation—including cloud computing and social media—represents the No. 1 source of disruption. Investors say business models are the second greatest disruptive force, while CEOs say it is changing customer behaviors.

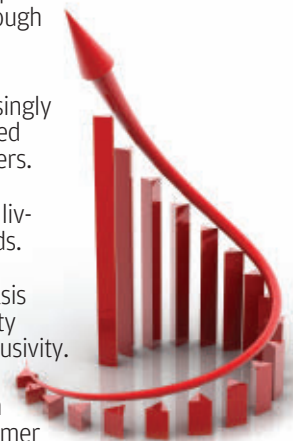
Despite acknowledging these challenges, many CEOs appear ill-prepared to address disruptive change in their organization, according to the EY research. Only half of chief executives surveyed in the firm's

THE FUTURE OF MARKETS

Recent analysis identifies several “megatrends” that may shape consumer markets through 2030.

- Increasingly connected consumers.
- Ethical living trends.
- Emphasis on quality and exclusivity.
- Growth of consumer spending in Asia.
- Reinvention of the shopping experience.

Source: Euromonitor International, Megatrends



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



95%

OF IT SECURITY PROFESSIONALS

say machine learning is a critical component of a cybersecurity strategy.

87%

REPORT THEIR ORGANIZATIONS ARE USING ARTIFICIAL INTELLIGENCE (AI)

in their cybersecurity strategy.

75%

SAY, WITHIN THE NEXT THREE YEARS, their company will not be able to protect digital assets without AI.

“There is no doubt about AI being the future of security, as the sheer volume of threats is becoming very difficult to track by humans alone,” says Hal Lonas, chief technology officer at IT security company Webroot.

Source: Webroot and Wakefield Research, Game Changers: AI and Machine Learning in Cybersecurity

CEO Imperative report say they are well-positioned to leverage disruptive change and opportunity. Just 54 percent say they own the company’s disruption agenda, and only 43 percent rate their organization as “good” at investing in exploratory, long-term return-on-investment projects.

Even fewer CEOs (39 percent) assign their company a “good” or “very good” rating when it comes to making internal risk capital available and developing autonomous

innovation units, and less than one-third rate these capabilities as “better than good.” According to the research, these two areas represent the greatest organizational weaknesses in terms of leveraging innovation capacity. Nonetheless, the study’s authors note that 67 percent of institutional investors say they want companies to undertake disruptive innovation projects, even if the projects are risky and do not deliver short-term returns. — **D. SALIERNO**

CONTROL REINFORCEMENTS

Scandals are leading Japan’s manufacturers to shore up internal controls.

Following recent scandals involving some of Japan’s biggest manufacturers, about 90 percent of companies surveyed say they are concerned the incidents will negatively affect the nation’s reputation for manufacturing excellence. More than one-fourth of those companies say they are highly concerned, according to a Reuters Corporate Survey of more than 500 large and mid-sized Japanese companies, conducted by Nikkei Research.

Last year, Japanese manufacturing suppliers Kobe Steel Ltd., Mitsubishi Materials Corp., and Toray Industries Inc.

admitted fabricating product data. Separately, Subaru Corp. announced it would strengthen compliance and oversight after admitting in October that uncertified technicians had performed final vehicle inspections for the past 30 years. In a December report to the Japanese government, the company said the importance of the inspections had not been appreciated by management and staff.

Like Subaru, nearly half (44 percent) of responding companies say they are working to strengthen quality controls in response to the scandals. Steps include enhancing compliance training, improving oversight of product controls, reviewing regulations, and conducting surprise inspections. — **T. MCCOLLUM**

BOARD PRIORITIES

Most corporate directors say significant industry change—driven by technology disruption, consolidation, and shifting regulations—will have the greatest effect on their companies in 2018, according to the

An NACD survey reveals top concerns and challenges for corporate directors in 2018.

National Association of Corporate Directors’ (NACD’s) 2017-2018 Public Company Governance Survey. Other



top trends are business model disruption, changing global economic conditions, cybersecurity threats, and competition for talent.

“A close look at this survey reveals that today’s directors are facing unprecedented challenges, demands, and

IMAGES: TOP, MAKSIM KABAKOU / SHUTTERSTOCK.COM; LEFT, NAITAPOL SRITONGCOM / SHUTTERSTOCK.COM

expectations that amount to a new mandate for boards,” NACD President and CEO Peter Gleason says. The survey of 587 corporate directors representing 520 public companies gives insights into directors’ 2018 outlook on key business trends and board priorities.

Among those concerns is the impact activist investors have on strategic goals. The survey notes that companies under pressure from activist investors to deliver short-term results are more likely to report compromised long-term strategic goals.

Of note is the disconnect in the board’s understanding of culture beyond the executive’s perspective. Eighty-seven percent are very familiar with the tone at the top, but only 35 percent of directors say they have a good understanding of the health of the culture at the middle levels of the organization and 18 percent know its strength at the lower levels. Seventy-nine percent of directors report they are confident in management’s ability to sustain a healthy corporate culture during periods of significant performance challenges. However, 92 percent rely on the CEO for information about organizational culture. Fewer hear from specialist functions—internal audit (39 percent), compliance and ethics (30 percent), and enterprise risk management (20 percent)—that possess deeper and more independent perspectives.

—S. STEFFEE

REGULATION READY?

Auditors can help their organization navigate the European Union’s General Data Protection Regulation, coming in May, says Donna Gracey, data protection officer and internal auditor for the U.K.’s Punch Taverns.

How can internal audit help the organization understand the requirements of the General Data Protection Regulation (GDPR)?



The most important part auditors can play is to offer expertise, where possible. In my company, I am responsible for internal audit and data protection; therefore, it was important that I understood GDPR as much as possible and how it would affect the way we do things. I then raised awareness across the business to help each department understand what it needed to do to be fully compliant with the new regulations.

Another important part was to make people comfortable enough to share any concerns they had with existing procedures so we could correct those while working toward compliance. I would advise internal auditors to keep abreast of new developments with GDPR, as they can play a key role in helping the data protection officer (if there is one) raise awareness of the new law, talk about potential risks, identify gaps in the company’s compliance program, and help to drive change within the organization. Though we have come a long way in 18 months, we still have a way to go. Now that everyone is talking about data protection and GDPR, the project has been helped immensely.

NEW YEAR, NEW PCAOB BOARD



The U.S. Public Accounting Oversight Board (PCAOB) has an all-new look. William Duhnke III was sworn in as PCAOB chairman last month and four new board members have been appointed by the U.S. Securities and Exchange Commission.

Incoming chairman seeks to advance “sustainable” audit quality.

Duhnke most recently was the majority staff director and general counsel to the U.S. Senate Committee on Rules and Administration. He replaces James Doty, who was appointed chairman in 2011. Upon taking office, Duhnke said his goals are “developing a collaborative and consensus-based approach to the PCAOB’s programs and operations and advancing sustainable audit quality that benefits the capital markets.”

Joining Duhnke on the board are J. Robert Brown, previously a law professor at the University of Denver; Duane DesParte, recently retired as senior vice president and corporate controller at Exelon Corp.; Kathleen Hamm, formerly global leader of securities and fintech solutions at Promontory Financial Group; and James Kaiser, most recently a PwC partner. —T. MCCOLLUM

Back to Basics

BY YULIA YEVLANOVA EDITED BY JAMES ROTH + WADE CASSELS

SMALL BUT EFFECTIVE

With the right tools and planning, small audit shops can be just as successful as their larger peers.

Because of a scarcity of resources, small audit functions face several risks, including the inability to meet expectations of the board and senior management, failure to achieve objectives, and lack of continuity. But they can develop strategies and use tools to overcome these obstacles, taking advantage of opportunities related to their size.

Work With Stakeholders

Internal auditors in small audit functions should identify departments in their organizations that can add value to internal audit and assist it in leveraging scarce resources—departments such as risk management; compliance; environment, health and safety; security; legal; IT; governance and strategy; resource planning; and quality assurance. Building long-lasting relationships with these areas allows internal audit to be aware of identified risks and

understand the processes and controls put in place to mitigate such risks.

Involving experts from other departments on individual engagements brings expertise that internal auditors lack for a specific project (IT, legal, engineering, etc.) and provides the experts with insight about internal audit methods and the types of information internal auditors are looking for. The experts should be independent of the audited area, supervised, and approved financially by management to provide assistance.

Internal audit also may consider asking someone within the organization to review audit work—someone who has knowledge and experience, particularly in governance, risk management, and audit practices, such as a former internal auditor or an employee who is a member of an audit committee in another organization. Documentation of such reviews should be kept.

There also should be cooperation with external auditors, peer reviewers, hired consultants, and regulatory authorities. Even if internal audit work is not used by external auditors or consultants, the chief audit executive (CAE) should keep in touch with them to discuss risks and potential flaws in the system of internal controls, as well as best practices. Knowing the plans and areas to be covered by external reviewers, an internal audit function can reallocate resources to other risk areas. The function may benefit from the findings in those areas addressed by external stakeholders and reviewers when they are interpreted through the prism of the whole organization.

Leveraging the knowledge, experience, and best practices of industry peers and local IIA chapters also can help resolve complicated issues. Through interaction with such groups, internal auditors can get access to valuable resources, such as

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



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

presentations and manuals, templates of audit programs, and other internal audit documentation.

Prioritize Tasks

It is important that the CAE carefully prioritize internal audit work by considering audit activities included in the annual audit plan, emerging high-risk and sensitive issues, urgency of requests, and availability of internal audit staff and staff within the audited area.

Limited time can be prioritized by using internal audit software and software used by other departments for data analysis and reporting, as well as templates developed for various tasks and procedures. This allows internal audit to spend more time solving complicated audit issues instead of performing manual routine tasks.

Flexibility can be increased by reserving time for consulting and investigative engagements and other activities not known in advance. Internal audit also could consider performing audit engagements in two stages: interim and final. During the interim stage, internal auditors perform a preliminary review of available information and systems and discuss questions and concerns with audit clients to learn about additional resource needs or how much unplanned time auditors may require during the final procedures. Practitioners then can provide some insight to clients about what to expect during the final audit stage and contribute to better management of the budget and uncertainty.

It also is important that internal auditors participate in meetings on strategic initiatives early on, which enables them to add greater value to governance processes, risk assessments, and internal control improvements. Auditors can prioritize their limited time by attending the most crucial meetings and rely on the review of the minutes from others.

If internal audit still cannot manage all the requests or does not have the expertise to address some of them, it should consider cosourcing. This is beneficial when specialized expertise or software is needed, but not available, in an organization; multiple requests have to be addressed urgently; the value expected from the project can be leveraged; and additional budget is available for hiring temporary employees. Interns or cooperative education students can perform less complicated tasks, especially during the busy season, or be involved in administrative tasks for the internal audit function, which can assist in managing a small budget. However, appropriate safeguards should be put in place when providing temporary employee access to internal audit information.

Communicate

A CAE should be open and work closely with the board and senior management when analyzing the resource needs of the audit function so they understand the existing trade-off

between the resources, internal audit objectives, and compliance with the requirements of The IIA's International Professional Practices Framework. If limited resources cause nonconformance with the *International Standards for the Professional Practice of Internal Auditing*, the board and senior management should be informed and should agree to this outcome. It is crucial that an open discussion among the CAE, board, and senior management happens regularly as expectations and objectives change, which leads to changes in resourcing needs.

Maintaining continuous communication with various departments in an organization can be done through planning and close-out meetings during engagements, collecting feedback in surveys, and organizing workshops and other training. Investing time in continuous communication can pay off for internal audit in the long run.


Develop a Continuity Plan

Continuity, consistency, and quality of work can be difficult to maintain, especially if there's high employee turnover. The internal audit charter, policies, procedures, and manuals enable the function to comply with the *Standards* and improve consistency of audit work. The same is true for templates that are used during internal audit projects, management of the internal audit function, and reporting to the board and senior management. Well-organized records and information management assist in preserving these tools for continued use.

Another element of a continuity plan, as well as a requirement of the *Standards*, is the assessment of a quality assurance and improvement program (QAIP). A thorough QAIP reduces the risk of nonconformance with the *Standards*. To improve the QAIP, small internal audit functions can involve peer organizations to identify common flaws in it.

Activity calendars for each staff member that include important activities performed annually by each position and due dates (such as audit planning, QAIP, reporting to the board and senior management, etc.) also can be used. Such calendars will help provide directions for existing staff members, develop the expectations for newcomers, manage budgeted time, and monitor performance against targets.

Set Realistic Expectations

Though an audit function may be small, it does not mean it cannot be effective. With the right tools and focus, small audit functions can meet the expectations of the board and senior management, achieve objectives, and maintain continuity. By setting realistic expectations and being flexible and efficient, small functions can be just as successful as their larger peers. 

YULIA YEVLANOVA, CIA, CPA, CGA, ACCA, is an internal auditor at the University of Regina in Saskatchewan.

BY STEVE MAR

BRINGING CYBERSECURITY INTO THE FUTURE

Internal auditors should consider whether CARTA is a smarter approach to addressing information security risks.

One can get overwhelmed reading about data breaches such as last year's massive Equifax incident, which may have exposed 145.5 million customer records. The December Identity Theft Resource Center Report lists other big breaches in 2017 at America's Joblink Alliance (5.5 million records), Sonic Drive-in (5 million), Dow Jones (2.2 million), Schoolzilla (1.3 million), and Washington State University's Social & Economic Sciences Research Center (1 million). Accenture's 2017 Cost of Cyber Crime Study notes such incidents increased 23 percent and cost on average \$11.7 million in 2017. These findings suggest that current security methods are unsustainable.

Against this backdrop, Gartner introduced an alternative approach to cybersecurity, the Continuous Adaptive Risk and Trust Assessment (CARTA), as

part of its Top 10 Strategic Technology Trends for 2018 report. The CARTA approach calls for real-time risk assessment and making trust-based decisions. This contrasts with previous information security strategies that revolved around periodic risk assessments and controlling users through single sign-on authentication. "Existing security decision-making based on initial one-time block/allow security assessments for access and protection is flawed," the Gartner report explains. "It leaves organizations open to zero-day and targeted attacks, credential theft, and insider threats." In this new paradigm, internal audit needs to determine how it will respond to the CARTA approach.

A Big Change in Thinking

The CARTA approach could become the model for organizations that are adopting the Development and Operations (DevOps)

approach for rapid application delivery. It relies on using application program interfaces (APIs) for automation, moves away from simple rule-based systems, and puts greater emphasis on detection and response vs. prevention. At its core is a three-pronged strategy combining deception, continuous authentication, and a development security operations (DevSecOps) mindset.

That requires a big change in thinking about cybersecurity. "CARTA is good at the framework level, but the implementation of it will require a major shift for vendors, software developers, and the organizations, themselves," says Sajay Rai, CEO of Securely Yours LLC in Bloomfield Hills, Mich. "Most organizations will have to deploy a different set of tools, technologies, people, and processes."

Although CARTA can be a helpful approach, it should not be viewed as a

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



TO COMMENT on this article,
EMAIL the author at steve.mar@theiaa.org

standard against which to audit, says Jon West, chief information security officer at Kemper Corp. in Jacksonville, Fla. “Organizations should work toward maturing to that level, but many have a long way to go,” he explains. “The important thing is that business, IT, security, and audit leaders understand that security-by-design has to be embedded into strategies and requirements.”

Deploy Deception Security Technology

Today’s most common cybersecurity approach aims to block all unauthorized users. To this end, organizations deploy firewalls, divide the organization into different segmented networks, and set up demilitarized zones.

A “deception” approach assumes some unauthorized user eventually will enter the organization’s network, despite efforts to prevent bad traffic. When that happens, the organization uses deception to lure intruders to a special server containing files that appear to be valuable information. In reality, the server tricks the intruder into clicking on the files, which alerts the information security function to take action against the unauthorized user.

In assessing CARTA, internal audit needs to determine whether the information security function plans to deploy or is already using deception. Auditors should assess the possibility of a CARTA strategic change and the new risks it may bring.

Establish Continuous Authentication

Continuous authentication applications constantly monitor the user from login to sign out. Some of these solutions include deploying keystroke analysis and touch- or mouse-motion dynamics. The idea is to identify a user based on “who you are,” including biometrics and face recognition, rather than “what you know” such as a password.

Some organizations use voice recognition to authenticate users and alert the information security team when it detects a significant variance. For example, Capital One Bank allows customers who have Amazon’s Echo personal assistant to say: “Alexa, ask Capital One, what’s my balance?” or “Pay my credit card.”

Using various behind-the-scenes authentication methods enables continuous authentication of the user. However, this new technology can be challenging to deploy and raises privacy questions for some users. How will internal audit adapt its governance, risk, and control assessment to this new type of authentication?

Create a DevSecOps Approach

The demand for innovation and delivering technology faster leads many organizations to use a DevOps methodology to develop and deploy applications into operations. With

DevOps, organizations seek to align technology with the business objectives and deploy new software releases faster.

CARTA inserts security into the DevOps model. This approach begins by making security people-centric and giving developers responsibility for security. Developers use automated tools to implement security during the development and testing of applications, and information security team members collaborate at key points during the process.


The challenge for internal auditors will be assessing the effectiveness of the DevSecOps approach. Will auditors require DevSecOps monitoring tools? Will IT auditors attend stand-up meetings and perform code reviews?

Internal audit can take three high-level steps to assess the DevSecOps approach:

1. Determine where the organization is heading strategically with cybersecurity. Is it taking a CARTA approach? This means the auditor has a seat at the table when innovative strategies are under discussion.
2. Assess the risk to successfully deploying deception technology. Internal audit should communicate with the chief information security officer to identify whether deception security is planned.
3. Review the benefits and cost for continuous authentication. Beyond costs and benefits, auditors should learn and become familiar with how continuous authentication works.

New Approach, New Methods

With many organizations already deploying CARTA, it could become the future of cybersecurity alongside the U.S. National Institute of Standards and Technology’s (NIST’s) Cybersecurity Framework and NIST 800-137: Information Security Monitoring, and Microsoft’s outcome-based security. Before deploying CARTA, organizations need to prepare themselves, says Ravi Raghavan, vice president of Coalfire, a Westminster, Colo.-based cybersecurity advisory firm. “Risk management is most effective after first conducting initial risk identification, prioritization, and triage exercises,” he says. “You have to have a house to stand in before you can continuously improve and repair it.”

In this environment, internal audit needs to collaborate with its information security counterparts to research and consider the CARTA approach and the new risks it may bring for their organization. Moreover, internal audit will need new audit methods and skills to address CARTA, and assessing the related governance, risks, and controls may be challenging. Getting started now represents the important first step. 

STEVE MAR, CFSA, CISA, is an adjunct professor in the Albers School of Business and Economics at Seattle University.

A New Look at Internal Auditing.



Introducing the Audit Intelligence Suite:

Benchmark | Assess | Survey

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

Learn More

www.theiia.org/AuditIntelligenceSuite



AUDIT EXECUTIVE
— CENTER® —

Risk Watch

BY JAMIE HOELSCHER EDITED BY CHARLIE WRIGHT

TAKING THE LEAD ON BLOCKCHAIN

As the technology behind Bitcoin finds new uses, internal auditors must assess how the risks may impact the organization.

Internal auditors are no strangers to change, and change continues to transform even the most traditional of processes. The latest revolutionary innovation is blockchain. Initially the technology underlying digital currencies such as Bitcoin, blockchain is beginning to change processes across many industries.

Like all new technologies, blockchain may produce innumerable new risks. Yet ultimately, it has the potential to help manage and mitigate many traditional audit risks. Internal auditors need to understand how blockchain may change business processes, determine the risks to the organization, and revisit audit processes and procedures to leverage the technology in their work.

How It Works

A blockchain is effectively a type of decentralized database known as a distributed ledger. Unlike traditional

databases, blockchains have no sole administrator. As each transaction is recorded, it is time-stamped in real time onto the “block.” Each block is linked to the previous block, and each user has a copy of that block on his or her own device. That process effectively creates an audit trail.

Blockchain is most notably used for transactions involving the buying or selling of digital currencies. Although the electronic encrypted audit trail is one by-product of the underlying technology of interest to internal auditors, another interesting side effect of the process is an accounting methodology called triple-entry accounting. Modern financial accounting is based on double-entry bookkeeping dating back to the 1400s. With triple-entry accounting, all entries for a given transaction are made to the blockchain to verify and document receipt of the transaction. Thus, triple-entry accounting

blends traditional double-entry accounting with third-party validation. As such, this methodology potentially could vastly alter traditional accounting processes and the subsequent control activities, risk assessment, and monitoring activities.

Impact on Audit Process

Often, internal auditors must catch up with technologies that are already in place, making modifications to the existing audit plan arduous and further emphasizing the need for a dynamic and adaptable audit plan. The complexity and incremental cost associated with blockchain implementation creates additional risk to the organization, making it vital that auditors are involved from inception and not just after implementation when a final process must be audited. Other risks associated with blockchain include scalability constraints, new privacy and security risks, and the need

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

IIA Training Stations

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



Learn From The Leader.

.....
IIA TRAINING – ALL PLATFORMS OPEN

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

Schedule training on a platform perfect for your station www.theiia.org/Training





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

to consider new regulatory requirements, many of which have not yet been promulgated.

Historically, auditors have been tasked with verifying the management assertions of existence, valuation, rights and obligations, completeness, and presentation and disclosure. The use of a distributed general ledger virtually eliminates the possibility of altering transactional data or inputting fictitious data, as the encrypted signatures of both parties involved in a given transaction are required.

Even with recent media coverage of digital currency hacks, the supporting technology underlying blockchain continues to be touted as “tamper-proof,” “validated,” “secure,” and “private.” Hacks are possible on applications that use blockchain, just as on an organization’s intranet. However, for a hack or data leak to occur, an attacker not only has to concurrently hack each user on the network, but also bypass encryption. Such an intrusion would be highly visible to those on the network. Internal auditors must perform comprehensive risk assessments to determine the likelihood, magnitude, and nature of potential threats as well as the appropriate preventive, detective, and corrective controls.

In addition to the data being more secure and valid, using a distributed public ledger gives auditors access to

from blockchain may enable internal auditors to focus on other high-risk areas such as internal control, compliance, or operational audits.

Audit Implications

With the advent of blockchain, the nature of audit work may change pervasively. Potential changes to consider include:

- *Systematically less reliance on paper documentation that can be altered or falsified easily.* Matching and vouching to test for existence and appropriate valuation may largely be outdated, as auditors will have easy access to transactional data that already has been mutually agreed upon and verified by an independent third party.
- *Differing cybersecurity risks and controls.* As the use of blockchain makes data available to everyone on the network, both physical and logical access controls will be more important than ever. In addition, use of a distributed public ledger can decrease the risk of successful computer attacks and may increase the visibility of attacks. The increased visibility elevates the importance of an organization’s incident response plan.
- *More involvement in creating new processes based on blockchain technology.* As recent publications from the Big 4 firms note, the reliance on blockchain technology

may require auditors to collaborate with IT professionals and raise the demand for auditors with IT expertise. Subsequent documentation of new processes and changes to old processes are key controls that auditors should not overlook. Over time, the use of blockchain may lead to increased stan-

dardization in both business processes and audit processes across industries as best practices emerge.

Efficiencies from blockchain may enable auditors to focus on other high-risk areas.

transactional data needed for the audit in real time, thus allowing for more continuous auditing. While continuous auditing has the potential to enable auditors to be more efficient, proactive, adaptive, and forward-looking, internal audit departments must explore the impact continuous auditing may have on existing audit programs and the potential disruption to the traditional audit cycle. Specifically, auditors must consider how it could impact scheduling, planning, and the actual collection of audit evidence.

While blockchain would in no way be a substitute for U.S. Sarbanes-Oxley Act of 2002 control testing, it could greatly increase the efficiency of traditional audits, creating a more uniform and highly verified audit trail from which to work. The improved quality of data and fewer reconciliations can potentially reduce the amount of work necessary throughout the year. Auditors may be able to conduct more work remotely, because less fieldwork will have to occur at the client’s site. Moreover, efficiency gains

Risks and Rewards

To prevent or lessen the risk of crisis that often precedes imminent change, internal auditors must stay abreast of emerging technologies such as blockchain. Yet, as with many new technologies and processes, blockchain may present a steep learning curve for auditors. Understanding the underlying technology of a distributed public ledger can enable auditors to assess the new control environment and new risks to the organization. In this way, internal auditors can be change agents who help mitigate the negative risks that all too often accompany the rewards associated with any new technology. [la](#)

JAMIE HOELSCHER, PHD, CIA, CFE, is an assistant professor of accounting at Southern Illinois University Edwardsville.

Fraud Findings

BY GRANT WAHLSTROM EDITED BY BRYANT RICHARDS

THE LOYALTY PROGRAM SWINDLE

Unscrupulous employees reap the benefits of loose controls in a company's promoter program.

Solarstar is a solar panel company with annual revenue of \$4 billion and a rapidly growing promoter program. Its commissioned sales representatives were encouraged to sign up small businesses and sole practitioners as promoters. Promoters distributed company designed and authorized literature (a one-page description of Solarstar's products and services) to potential customers and clients, who would call a dedicated phone number on the flyer and use a unique code associated with the promoter to obtain a quote. If a purchase was made, the promoter got a referral fee and the sales representative received a commission.

The promoter program was growing fast, and field management was ecstatic as it was thought to be opening a new sales channel. One afternoon, one of the more successful promoters contacted a Solarstar online moderator with a

request to be assigned to a new sales representative. The promoter alleged to be a 17-year-old girl, which caught the moderator's attention. Suspicions were raised and the transcript of the chat was sent to Solarstar's forensic audit manager, Robert Schull. After reviewing the transcript, Schull was determined to find out how a 17-year-old girl could have signed up as a promoter, let alone become one of the more successful promoters.

Schull first wanted to understand how the promoter program worked. He learned that it was outsourced to King Enterprises (KE), a small business run out of a strip mall in New Jersey. KE maintained a website that advertised the program and recruited potential promoters. The website had an online chat capability (that the alleged 17-year-old engaged) where current and potential promoters could ask questions or get help resolving concerns. Every

week, Solarstar bulk paid KE for all closed promoter sales. KE then facilitated payment to the promoters. KE also was responsible for submitting 1099s to the U.S. Internal Revenue Service (IRS) and transferring funds to state agencies in the event a promoter did not cash the referral check timely.

Initially, Schull focused on the promoter registration process. He went to KE's website and signed up as a promoter by entering his name, address, phone number, and email address. Schull waited a few hours and received notification that he was now a registered promoter. Upon inquiry, he discovered there was no validation process to confirm the identity of the individuals registering as promoters. A review of the promoter database revealed names that were, in fact, companies. For example, multiple promoters alleged to be Comcast, Disney, Dominos, or Time Warner Cable. KE only required

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



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

LESSONS LEARNED

- » Promoter program terms and conditions should be reviewed to determine the criteria for becoming a promoter and how the employee and promoter earn a referral fee. Determine how the organization validates the authenticity of the promoter and the sale.
- » Contracts with vendors should be reviewed to verify that they have a right-to-audit clause. From time to time, the right-to-audit clause should be executed. An effective audit technique is to compare an employee database to the vendor database by name, address, and phone number. Phone numbers are particularly effective in finding duplicates.
- » Require all employees with the potential to interact with vendors to complete a conflict of interest form. Prompt employees to update their conflict of interest form annually. But remember, conflict of interest forms are useless unless someone reviews the disclosure of conflicts and follows up with the employees.
- » Pay promoters with gift cards instead of cash. This should help deter individuals from trying to turn your promoter program into a small business.

a Social Security number if the promoter exceeded \$600 in referral commissions, which is the minimum requirement established by the IRS for submitting Form 1099.

Schull interviewed Mary St. Croix, the sales representative associated with the 17-year-old girl. She admitted that the promoter was her ex-boyfriend and not a 17-year-old girl. Allegedly, the ex-boyfriend was a married undocumented immigrant (purportedly with a criminal background) who used an alias and his son's Social Security number. He cashed his promoter referral checks at the local gas station. St. Croix provided a copy of a police report attesting to his violent nature, as well as the relationship. Her employment was soon terminated and the promoter was removed from the program.

As the contract between Solarstar and KE was about to expire, Schull next examined the program, itself. In interviews with employees who worked closely with KE, one employee alleged KE was keeping the funds from uncashed checks for promoters rather than transferring the checks to the appropriate state authorities. Schull's request to audit KE's books was rejected on the grounds that there was no right-to-audit clause in the existing contract, which was confirmed after review.

Schull next turned his attention to the promoter network. Based on the initial investigation, he believed that if sales representatives could work with a fabricated promoter, then they must be able to sign up a spouse, relative, or co-worker. He used data analytics to compare employee names, addresses, and phone numbers to the promoter database. Much to his surprise, dozens of employee names were in the database. Some employees set up their spouses, fiancés, brothers, and sisters.

One entrepreneurial employee maximized the program's potential by signing up his not-for-profit company and his church, and then signed up subpromoters (his relatives) under the church. A promoter could sign up a subpromoter and generate a sales commission for the sales representative and a referral fee for the promoter and the subpromoter, who in this case were all the same person. Essentially, the sales representative created a Ponzi scheme generating commissions and referral fees for himself, his company, his church, and his family.

Joe Smith, Solarstar's finance director, requested a meeting with Schull when he learned that revenue from customers signing up through the promoter program had slowed considerably. At the rate it was going, Smith calculated that the program would lose approximately \$7 million each year. Smith's analysis of sales and Schull's field investigations revealed that dozens of sales were being made to customers living in low-income apartment complexes and trailer parks by unscrupulous sales representatives and their promoter friends. In some cases, sales representatives signed up promoters who were unemployed and had them knocking on doors or placing flyers on cars in mall parking lots.

Schull and Smith took their findings to management. Ted Spicoli, the vice president of sales and in charge of the loyalty program, refused to believe that the fraud in the program was as prevalent or widespread as Schull and Smith stated. He challenged Schull's findings and Smith's analysis. During one contentious meeting, he even challenged Smith's ability to perform basic math. Months passed, and more money was lost until finally the program was shut down. KE's contract was not renewed, and Spicoli was fired.

The promoter program was redesigned and launched as a friends and family program encouraging existing customers in good standing to refer a sale. Compensation was changed so sales representatives received a commission and the existing and new customer would split the referral fee, which was no longer paid in cash, but in gift cards. After six months, the new program was generating good customer sales without a single incident of fraud detected. [\[a\]](#)

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

Board

Internal audit and board alignment can best be achieved when each looks to understand the priorities and needs of the other.

SIRTRAVELALOT AND MINERVA STUDIO / SHUTTERSTOCK.COM



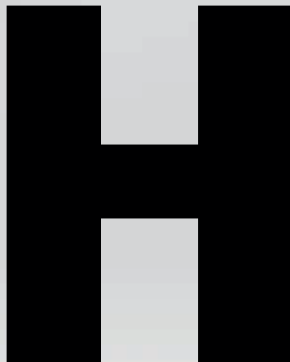


Matters

Arthur Piper

Having a sound relationship with the board is crucial if internal audit functions are to serve their organizations well and provide effective assurance. Whether chief audit executives (CAEs) report directly to the board or, more likely, to an audit committee, it is vital that the two sides share an informed understanding of internal audit and its role and purpose within the organization. That is why educating the board about the level and nature of assurance internal audit provides is an important part of any CAE's role.

While that is an easy principle to grasp, achieving it in practice can be a difficult and prolonged journey for both sides. Explaining what internal audit can do and how the function should be positioned in the business is likely to be unhelpful, unless it is done in the context of the board's real-life needs. "CAEs should be thinking about putting themselves in the shoes of the board members, and understanding what is on their agenda and why," says Ninette Caruso, CAE





MONKEY BUSINESS IMAGES / SHUTTERSTOCK.COM

An element often missing from such conversations is internal audit's feedback on the effectiveness of the corporate governance framework.

at Discover Financial Services in Riverwoods, Ill. Boards are more likely to be concerned with business issues such as profitable growth, dealing with competitors, net profits, and complying with pressing regulatory issues. If internal audit is not engaged in those areas, trying to educate the board about assurance is likely to feel too abstract and disconnected from the business.

BOARD PERSPECTIVE

As internal audit begins to provide specific value and advice to the board in those parts of the business where it has genuine concerns, Caruso says it will be effectively educating the board about what true risk-based internal audit means to the organization by demonstrating the type and level of assurance it can provide.

In doing so, internal audit will be greatly appreciated and recognized for it.

“Let’s try to understand where the board is coming from and not waste time trying to add value to, say, a compliance audit if the board is not really interested in that area,” Caruso says. “Instead, the internal audit function needs to focus on perhaps two main issues on the board’s agenda at that particular point in time and to put all of its efforts into those areas.”

Getting issues onto the board’s agenda that internal audit feels are important, but the board does not, can be more challenging. Caruso says it demands a level of storytelling that auditors are not often used to about what they have found and why that matters to the organization.

“Even if the board only wants internal audit to check the controls put in place by management and risk functions, internal audit can still play an educating role by standing back and looking at themes that emerge from the interaction between different parts of the business,” Caruso says. “Nobody may want that from internal audit until we bring it to them and they can see the value of it firsthand.”

A CLEAR UNDERSTANDING

Louis Cooper, chief executive of the U.K.’s Non-Executive Directors’ Association, a professional training and education membership organization based in London, understands how CAEs and nonexecutives think about each other. He agrees with Caruso when she

94% of CAEs surveyed in The IIA's 2018 Pulse of Internal Audit strongly agree or somewhat agree that the internal audit plan incorporates input from the audit committee.

says that CAEs often dive in, providing services that they believe the board will want without stepping back and asking some simple questions first—and listening to the responses.

As Caruso says, boards generally want to know what the key issues are and what the organization needs to do to respond to them. But building a picture of what the board wants can take time. “Internal audit often has a disjointed view of the board because of the limited contact it has with its members through various committees and because of the brevity of that contact,” Cooper says. “Quite often, internal auditors only get pulled into the audit committee to present their report, so they often don’t have ongoing dialogue with key board members, especially the audit committee chair.”

In addition, internal auditors are busy people, he says, concerned with delivering their audit plans. That is why it is important for CAEs to schedule time within the audit plan, itself, for relationship building. Internal auditors can use those meetings to both strengthen their understanding of the board and explain how the function can serve the organization’s broader needs.

“Having a clear understanding of the corporate governance framework within the organization enables people to connect the dots on the risks that have been identified in the organization,” Cooper says. “Internal audit’s knowledge of the organization and its related feedback on the effectiveness of the corporate governance framework is an element often missing from such conversations.”

If the CAE can help the board come to grips with the control environment and help ensure management takes more ownership over some of the control processes, it can promote a better balance of activity based on management fulfilling its role in the Three Lines of Defense model. That helps move internal audit away from

low-level controls testing and into a more strategic risk-based auditing, the internal auditor’s “holy grail,” which can, in turn, free time in the audit plan for big-picture audits or consultancy-style projects.

MANAGE EXPECTATIONS

Kristiina Lagerstedt, vice president, Audit and Assurance, at Sanoma in Helsinki, and a board member at Uutechnic Group, says internal audit departments can educate boards on the progress of big change projects. She has been working on information security and privacy readiness and maturity in preparation for the European Union’s stringent new General Data Privacy Regulation (GDPR), set to come into force this year. Because Sanoma is operating in the media and learning sector, getting the rules right is crucial.

“When GDPR was introduced, I noticed there wasn’t a common approach to privacy and information security within my company,” she said. She raised the issue, and the company decided to establish a steering group to oversee preparations for the changes with the CEO as chair.

“I took care of the agenda for the first year and a half, and we met twice a quarter,” she explains. Six months ago, when the steering committee agreed that the privacy and information security programs were up and running appropriately, it decided to meet quarterly and the agenda moved over to the chief information security officer. Lagerstedt is still involved, but with a smaller role.

“For a CAE, it is important to get involved in group-level change programs to ensure a common approach across businesses and countries,” she says. Lagerstedt’s main contribution was to keep the project moving and keep top management and the board up to speed on the progress made, the main risks faced and how they were being



“Internal audit often has a disjointed view of the board because of the limited contact it has with its members.”

Louis Cooper



“Let’s try to understand where the board is coming from and not waste time trying to add value to [an area it’s not interested in].”

Ninette Caruso

Building a picture of what the board wants can take time.



MONKEY BUSINESS IMAGES / SHUTTERSTOCK.COM

dealt with, and the maturity levels the business units had achieved on a quarterly basis.

“When you are pushing things forward and operating as a change agent (or consultant), it is sometimes confusing for people in the business to understand what the role of internal audit is and should be,” she says. While internal audit took a front-line role in the GDPR project in some respects, she aims to involve the business’ external auditors in the next audit to help reassert internal audit’s independence.

“Be brave in the tasks you take on,” she says. “Think about the company doing the right thing, but also keep in mind your and your team’s limitations to successfully manage expectations and not give promises you cannot keep.” She says continual education about what internal audit does and can do is key to success. “Remember to keep top management and the audit committee informed about

where you are, and what the next steps and most critical risks are,” she advises.

EXPLAIN THE STANDARDS

For David MacCabe, a longtime CAE and an internal audit consultant based in Austin, Texas, informing the board that the internal audit function is conducting engagements in line with the *International Standards for the Professional Practice of Internal Auditing* is on his list of the critical assurances the CAE should provide to the board.

“Some members of the board may have minimal experience in business operations, such as those in nonprofit organizations, and they may just be interested in the programs and the people they serve,” he says. “But even in corporate America, there are some members of the board who may not be sure what their full duties and responsibilities are—and what the appropriate questions to ask as a responsible board member are.”

Internal audit can help educate them about those duties and, in doing so, underline its own credibility and integrity by explicitly saying it adheres to these international standards, he says. “Even for experienced boards, it can be useful to demonstrate that you are committed to external quality reviews by independent practitioners so they will know you are a step above what they may have experienced elsewhere,” he adds.

BUILD RELATIONSHIPS

Effective communication and other interpersonal skills are crucial to achieving that goal and, while MacCabe says today’s auditors are generally more personable than in the past, there is room for improvement. In addition, The IIA’s many useful tools and publications can help CAEs inform and educate the board about leading practices for internal audit teams and audit committees.

56% of audit committees say internal audit can **maximize its value** by expanding audit plans on key areas of risks and related controls, according to KPMG's 2017 Global Audit Committee Pulse Survey.

IIA STANDARDS

Although The IIA's *International Standards for the Professional Practice of Internal Auditing* does not explicitly say that the internal audit function should educate the board, it can be inferred from the many ways in which auditors communicate and work with directors and management across the business. While there is obvious value in providing education as to the effectiveness of the governance processes within the organization, and the type of major risks change projects can bring about, does it make sense to try to educate the board about the *Standards*? After all, the *Standards* are meant to be the benchmark of audit quality.

"Effective communications enable the audit committee to work with internal audit leaders to better understand the internal audit process," Jim DeLoach and Charlotta Hjelm wrote in their 2016 CBOK Stakeholder Report, *Six Audit Committee Imperatives: Enabling Internal Audit to Make a Difference*. "To this end, directors should become more familiar with The IIA's International Standards."

Given the time constraints that both internal auditors and board members experience, is such a suggestion realistic or even desirable? According to evidence included in the report, the answer is yes. The quality and frequency of communication between CAEs and board members is greater among stakeholders familiar with the *Standards*, according to the report. Specifically, two out of three board members are familiar with the *Standards* to some degree and almost all—98 percent—see value in internal audit conformance.

"If audit committee members do not have adequate knowledge of the *Standards*, they should ask the CAE for more information about them and how internal audit is ensuring their conformance," DeLoach and Hjelm conclude.



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

He agrees with other CAEs that progress can be slow, and trust and respect need to be earned both by word and deed. Being proactive and available to management and staff in formal and informal settings can be a winning approach, MacCabe says. "It makes a world of difference to be open-minded, available, accessible, and approachable in the hallway, in the cafeteria, and wherever in the organization," he says. People are much more likely to share their concerns when you are friendly, and people get to know you.

He recalls one time when he brought a story he had heard through conversations with staff to a line manager. "The manager was worried I'd pass it on to his section head, but I gave him the option to act on it or not, and emphasized that it was not a complaint or concern, but an observation about something that may or may not be true," he says. Situations like


this can help form great relationships because the auditor is then viewed as being available to discuss issues and provide informal advice for control improvements or remedial actions.

"Building those relationships throughout the organization from the board to the frontline of the business is crucial," MacCabe says. "Management often asked me to pass things onto the board, and that can be done either in confidence, or openly as they choose. Everyone benefits."

COMMIT TO IMPROVEMENT

MacCabe says internal audit also must be committed to continuous improvement through internal and external quality assessments (refer to Standard 1300 series) and by continually updating its knowledge of leading internal audit and management practices, as well as business and industry trends. For that, quality assurance reviews are particularly

important—especially because they form a key part of conforming with professional standards. He says he worries that only 39 percent of survey respondents worldwide said they had such an external review, according to the Common Body of Knowledge (CBOK) 2015 Global Internal Audit Practitioner Survey.

"It's no use saying that we are professionals and then only being partly in conformance with our own *Standards*—that erodes our credibility," he says. He urges CAEs and all internal auditors to be committed to achieving and demonstrating the highest professional standards. In striving to do so, auditors will become a more respected and vital source of knowledge and education on assurance for everyone in the business—especially the board. 

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



The Biggest Risk is Falling Behind

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

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

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

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

- UMC Health System

"TeamMate+ reporting has significantly improved our process allowing us to provide more consistent and thorough analysis to management, auditees, and external auditors. We now have greater visibility across our audit projects."

- ORIX USA Corporation

TeamMate+

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

the CAE-CRO relationship

Chief audit executives and chief risk officers can collaborate in many ways to ensure the organization manages risks effectively.

Charlie Wright

As enterprise risk management (ERM) continues to mature in organizations around the world, it has become clear that there are many different approaches to implementing it effectively. However, one of the themes that continues to evolve is the interaction and relationship between the chief audit executive (CAE) and the chief risk officer (CRO). The roles of these positions are highly interrelated and interdependent. In fact, in many organizations the CAE *is* the CRO.

Both the CAE and CRO functions have unique opportunities to strengthen and improve the organization's risk management processes. For this to happen, the CAE and the CRO must work together closely, collaborate on many aspects of ERM, and coordinate with each other to eliminate redundant efforts and leverage the work of the two functions. To optimize ERM, organizations must first ensure the CAE and CRO functions are optimized individually and are integrated with each other appropriately.

WHO LEADS ERM?

In September 2017, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued an updated ERM framework, *Enterprise Risk Management—Integrating With Strategy and Performance*. The revised framework defines

ERM as “The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value.”

COSO’s updated guidance includes five components and 20 principles intended to help organizations navigate an increasingly complex governance, risk, and compliance environment. Today’s business world is driven by astounding advances in technology,

to ensure ERM is integrated into the culture and fabric of the organization. While the framework addresses some of these issues from a theoretical and strategic perspective, it leaves the implementation of specific activities up to each organization. Historically, the CRO or the CAE designed ERM based on the organization’s culture and the past use of internal audit and risk management processes. The updated guidance provides minimal information about which role should be performing specific ERM activities. Unfortunately, because the role of each of these functions is unclear and often depends on the personalities and skills of the individuals performing the jobs, many organizations end up with an ERM process that is not as efficient or effective as it could be.

The IPPF tasks the CAE with the responsibility for evaluating and improving risk management processes.

new media channels, and wireless access and mobile devices. The recent update repositions the framework in five ways:

- » Focuses on strategy.
- » Clarifies that ERM isn’t a standalone activity.
- » Advances the debate about risk appetite and tolerance.
- » Focuses on organizational value.
- » Provides a good mechanism for assessing an organization’s risk management practices.

The updated framework improves on COSO’s previous framework. It recognizes the impact of culture and strategy on an organization’s risk management practices, and importantly, it focuses on the creation, preservation, and realization of value.

However, the new framework does not provide guidance about which business function should be performing the wide variety of tactical activities that build the foundation for effective ERM. These activities include creating risk documentation, developing analysis and prioritization tools, designing governance and oversight processes, and establishing an ongoing process

THE CAE’S ROLE

The International Professional Practices Framework (IPPF) says internal auditing “helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.” The IPPF definition specifically tasks the CAE with the responsibility for evaluating and improving an organization’s risk management processes. The CAE should perform periodic risk assessments of the organization, create an organizational audit plan to evaluate the effectiveness of internal controls, and advise management on opportunities to strengthen and enhance controls.

Generally, this process requires development of an enterprise risk assessment that leverages risk assessments from various parts of the organization such as financial and operational processes, project management, IT, supply chain, and other business functions. It also may incorporate relevant risk assessments that management has performed related to

92% of financial institutions have a **CRO or equivalent** position, and 75% say the CRO reports to the CEO, according to Deloitte's 2017 Global Risk Management Survey.

strategy, operations, and compliance. The risk assessment process should result in a continually updated audit plan that includes engagements and tests that will allow internal audit to provide management with independent and objective assurance around the effectiveness of the organizational control environment.

The activities that allow internal audit to gather risk assessment data include discussions with management, reviews of policies and procedures, and surveys. To analyze the data, auditors must document and prioritize it based on the organization's needs. Many CAEs and management teams prefer the risk assessment data to be visualized by using charts, graphs, and heat maps. Internal audit's risk assessment analysis should culminate with an enterprise-wide risk register and a prioritized list of organizational risks that helps the CAE determine the optimal audit engagements for the organization.

THE CRO'S ROLE

The role of the CRO continues to evolve. CROs are responsible for implementing a consistent, integrated risk management framework throughout the organization. They oversee an enterprise risk assessment, articulate the risk appetite, and familiarize the organization, its shareholders, regulators, and rating agencies with the ERM program. Moreover, they ensure the organization has developed ways to mitigate risks to its objectives and create a risk-aware culture across the organization.

The CRO may function under a variety of names: head of enterprise risk management, head of risk, director of enterprise risk management, or director of risk. Whatever the official title, COSO's updated ERM framework indicates that the CRO often is responsible for providing expertise and coordinating risk considerations. Yet surprisingly, other than a brief mention,

the framework is silent regarding the CRO's role in ERM.

In practice, the CRO may have a background in insurance, disaster recovery, finance, IT, internal audit, compliance, or other disciplines. However, as ERM matures, more organizations are appointing CROs who have the ability to contribute at an executive level. As a strategic function, the CRO has become critical to helping organizations achieve their overall objectives by ensuring risk management functions are integrated across the organization and advising management about policy and decision-making.

The skills that make a CRO successful include the ability to advise executives and the board, collaborate with operational business leaders to identify risks, recommend opportunities to strengthen risk mitigations, and communicate with all levels of management and external stakeholders such as regulators. On top of these skills, CROs need a thorough understanding of the business. Managing risks is everyone's job, but the CRO must be

The CRO must be able to consolidate input from numerous broad disciplines and identify ways to add value.

able to consolidate input from numerous broad disciplines and identify ways to add value cost-effectively.

Much like the CAE, the activities that allow the CRO to execute his or her duties include performing enterprisewide risk assessments and leveraging risk assessments that are already performed in other parts of the organization. The CRO uses many of the same tactics such as discussions with management, interviews with subject-matter experts, analysis of risk metrics,



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

and surveys. The CRO also will create a prioritized list of risks.

The primary difference between the CRO and CAE roles in ERM is that the CRO participates in the organization's risk-making decisions and often is directly involved in facilitating risk decisions. On the other hand, it would be a conflict to a CAE's independence if

interactions with senior executives, the CAE and CRO must be able to communicate clearly, facilitate difficult meetings, and articulate complex issues concisely. Also, both roles require individuals who can conceptualize strategic issues and advise executives and the board about potential strategic risk management opportunities.

both functions significantly and eliminate unnecessary effort.

Collaborate on the Enterprise Risk Assessment Because both functions rely heavily on an enterprise risk assessment, the CAE and CRO should specifically identify the risk criteria that are important in their organization. By agreeing in advance on the content, layout, language, and approach to the risk assessment, both functions will be able to use the same information.

Coordinate on the Audit Plan The CAE should work closely with the CRO to ensure the organization's internal audit plan is designed to address organizational risks identified by the enterprise risk assessment. This can be accomplished by mapping and cross-referencing each of the planned audits to match the organization's risk profile. For example, if the risk function has identified cybersecurity as a key risk, the audit plan should consider audits relating to vulnerability assessments, penetration tests, and access controls. By ensuring the organization's most important risks have an independent and objective audit process, management and the board should have more assurance about the overall risk management process.

Address Potential Conflict or Rivalry Despite the critical nature of both roles, CROs and CAEs may disagree because of conflicting priorities, internal politics, and competition for resources. Open, frequent, and regular communication between the CAE and the CRO provides a good mechanism to address these issues.

THE CAE AS ERM LEADER

In many organizations, the CAE is heavily involved in ERM activities. These CAEs act as facilitators, working with risk leaders throughout the organization to document risks, execute risk surveys,

By collaborating, the CAE and CRO can have a combined effect that is more than the sum of their separate effects.

he or she were making risk decisions for the management team.

COMMON OBJECTIVES

The CAE and CRO share many common objectives. They both provide reasonable assurance that the organization is capable of achieving its objectives. To accomplish this, they evaluate the risk environment, ensure the management team is focused on the appropriate risks, and advise management about opportunities to improve risk management and comply with laws, regulations, and company policies.

The CAE and CRO both should be following the organization's structured risk management framework, including using common risk management language, interviewing the owners identified for each risk, and using the results of the analysis and prioritization aspects of the framework. By following the organization's framework, the two functions can reinforce the importance of risk management, educate business users about the process, and extend awareness of risk management to other employees.

To succeed in their roles, both functions require leaders who have strong interpersonal skills in addition to their technical expertise. In their

OPPORTUNITIES FOR COLLABORATION

Because of their common objectives, as well as similar and sometimes overlapping roles, the CAE and CRO must work closely together. By collaborating, the two functions can have a combined effect that will benefit the organization more than the sum of their separate effects and enable its risk management processes to operate more effectively.

Create Complementary Charters To ensure a good understanding of their roles, the risk and audit functions each need to develop charters describing their purpose, roles and responsibilities, reporting structure, and authority. The audit committee should review and approve the CAE's charter annually, while the risk committee, or its equivalent, should approve the CRO's charter each year.

Document Responsibilities Documenting which role should be responsible, accountable, consulted, and informed using a RACI matrix can help clarify and facilitate an improved understanding of each function's role. The combination of a charter and a RACI matrix can improve the effectiveness of

42% of audit committee members say their organization's risk management programs require substantial work, KPMG's 2017 Global Audit Committee Pulse Survey notes.

and chart and graph the risks after the management team has prioritized them. By facilitating and overseeing some of the ERM-related activities, the internal audit function can fulfill its responsibilities and add value in an integral part of the organization, as suggested by the Definition of Internal Auditing.


The IIA position paper, "The Role of Internal Auditing in Enterprise-wide Risk Management," presents a range of ERM activities an effective internal audit function should undertake. The most important safeguards that protect internal audit's independence and objectivity include documenting internal audit's role in the internal audit charter that has been approved by the audit committee, clarifying that management remains responsible for risk management, and ensuring internal

audit does not make risk management decisions. Moreover, CAEs should apply the relevant *International Standards for the Professional Practice of Internal Auditing*, including Standard 2120: Risk Management, 2010: Planning, and 2050: Coordination and Reliance. If the audit committee decides to use its internal audit function in an ERM leadership role, these issues should be discussed with the audit committee and the executives to ensure roles are clear.

Regardless of whether the CAE is leading ERM, the CAE should be intentional about developing an audit plan that integrates into the ERM program. One effective way to ensure adequate coverage is to organize the audit plan by ERM risks. Internal audit should identify the organization's key risks and determine the relevant audit programs

from the audit plan by each risk area. This approach provides comfort that the audit plan covers the key risks.

RISK PARTNERS

Virtually all industries face difficult challenges in managing risks in a complex, rapidly changing environment. That makes having effective risk managers in place a priority as organizations struggle to develop risk management programs that fit their specific circumstances. By working together, the CAE and CRO can improve risk awareness and develop a stronger overall ERM process that positions risk managers to meet the needs of their organizations. 

CHARLIE WRIGHT, CIA, CISA, CPA, is director, Enterprise Risk Solutions, at BKD LLP in Oklahoma City.

YOU *Are* INVITED

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

UPCOMING VISION UNIVERSITY SESSIONS:

Orlando
Feb. 26–March 1
Grand Bohemian Hotel
Orlando, FL

Philadelphia
June 19–22
Loews Philadelphia Hotel
Philadelphia, PA

www.theiia.org/VisionU

Where Your Path to CAE Success Begins

VISION UNIVERSITY



**AUDIT EXECUTIVE
CENTER®**

2018-0090

How's your

Emotional intelligence can help auditors build and maintain positive, productive relationships throughout the organization.

EQ?

J. Michael Jacka

Illustration by Sandra Dionisi

M

ark was dreading his meeting with Dave. His team had identified significant control issues in the new purchasing system—significant enough to have a negative impact on the system's stated objectives. Dave, the executive responsible for the system, had promised senior management it would not fail.

Mark walked into Dave's office after deciding it was best to get right to the point. "You've seen the draft of the audit report," he said. "It is apparent that the issues we identified reveal the program will not meet any of its agreed upon goals."

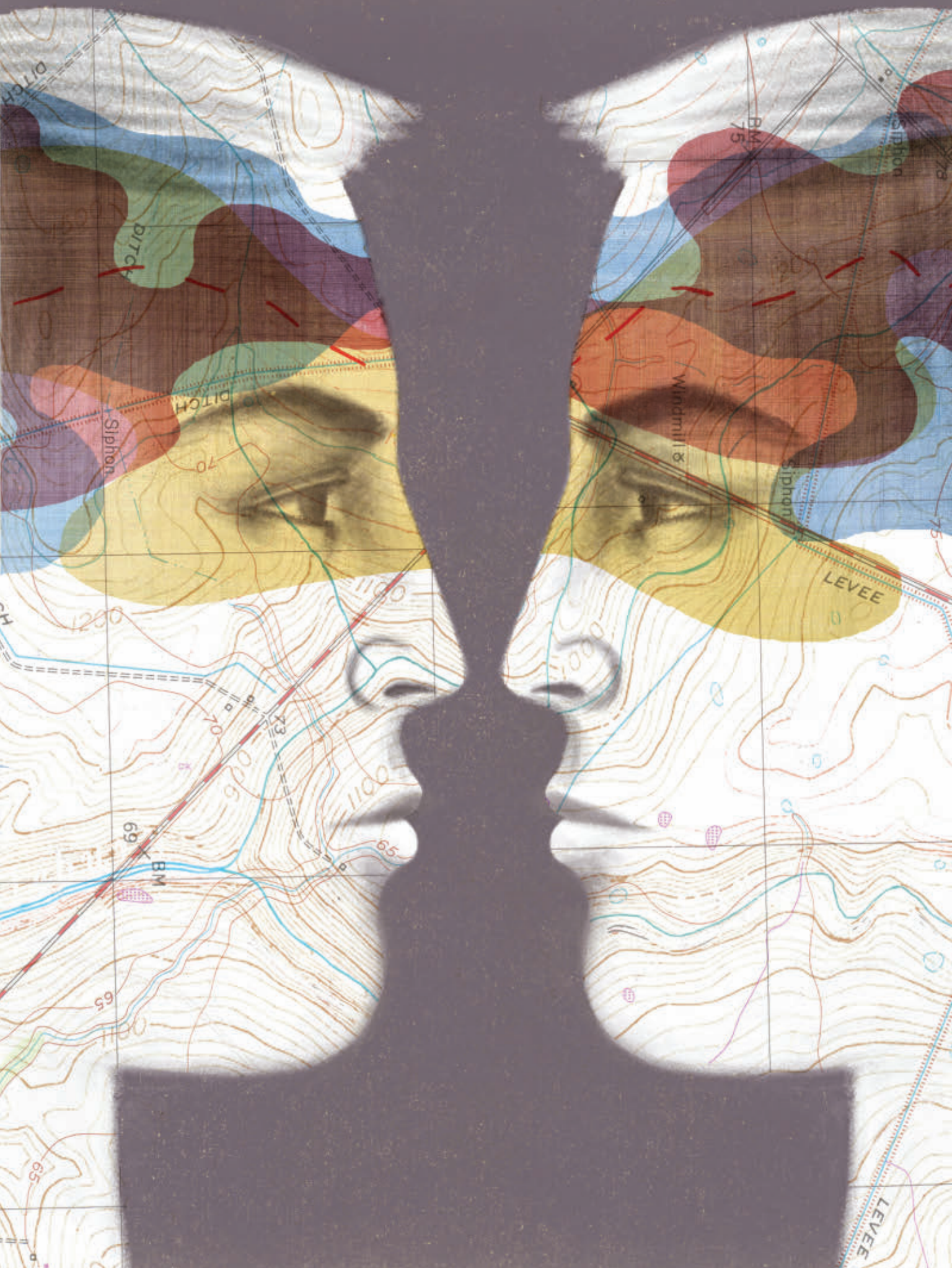
To Mark's surprise, Dave had no response—he just kept looking down at the report printout. But just as Mark was about to discuss potential corrective actions, Dave exploded. "I know how you auditors work," he yelled. "You come into an area you don't understand and dig until you find something wrong. You're just trying to

make a name for yourselves—you've always been out to get me."

Mark was taken aback but refused to ignore the attack on himself and his department. "We know exactly what we're doing," Mark snapped back. "And our only problem with you is that your project's failure will cost the organization a fortune." The conversation then quickly devolved into a shouting match, with fingers pointed and accusations of incompetence and poor leadership thrown about. Eventually, Mark was summarily dismissed from Dave's office.

As this scenario—based on real events—reveals, even the most well-intentioned meeting can go quickly awry. And while numerous reasons could be given for the communication breakdown, in essence both parties' emotions superseded rational discussion.

The scenario shows that, despite frequent emphasis on the need for internal auditors to possess analytical,



critical-thinking, and technical skills, the ability to establish effective interpersonal relationships is a much more important competency. An audit can be conducted with thorough attention to detail and accuracy, with meticulously supported findings, but one interpersonal misstep could shatter the entire process. Effective auditing requires practitioners to build and maintain positive relationships with clients and co-workers.

EMOTIONAL INTELLIGENCE

Understanding and managing one's emotions, as well as understanding the emotions of others, is fundamental to successful interpersonal relationships. The degree to which an individual possesses this ability is known as emotional intelligence—also referred to as emotional quotient (EQ).

EQ is best understood through the Emotional Competence Framework, developed by psychologist Daniel Goleman. Encompassing several practical skills that underlie EQ, Goleman's framework features a two-pronged structure consisting of personal competencies—how we manage ourselves—and social competencies—how we handle relationships. (For additional details on each of the framework components, see “The Emotional Competence Framework,” this page.)

Personal Competence These skills focus more on the individual than on the individual's interactions with other people. They involve the ability to stay aware of internal emotions while managing personal behaviors and tendencies.

- » *Self-awareness*—recognition of our emotions as they happen. An inability to notice one's true feelings as they occur leaves that individual at their mercy. Conversely, the ability to monitor these feelings as they occur allows better control of them.

When Dave attacks Mark, he responds without considering how his emotions have taken control. To keep the situation from escalating, Mark needs to understand the reasons for his immediate reaction before continuing the conversation.

- » *Self-regulation*—the ability to use self-awareness to better manage emotions (once they are recognized) and react appropriately. If Mark recognizes that anger is driving his reactions, he can pause, control his emotional response, and develop a response that does not escalate conflict.
- » *Motivation*—understanding the emotional tendencies

that guide or facilitate reaching goals. Any number of emotional motivations could be driving Mark's behavior—pride in the work his team accomplished, fear that the audit schedule would not be met, and as the meeting played out, anger over the impediment to completing the assignment. By understanding his motivations, Mark could ensure that his needs align with Dave's.

Social Competence These skills represent the ability to understand other people's moods, behaviors, and motives. They enable individuals to improve the quality of their relationships.

THE EMOTIONAL COMPETENCE FRAMEWORK

The Emotional Competence Framework describes the skills that comprise EQ. While no one can be adept at all of the skills listed, individuals with a high EQ will have strengths in some, spread across all five areas. The framework should be of particular interest to practitioners, as it covers skills required of top internal audit professionals.

PERSONAL COMPETENCE—HOW WE MANAGE OURSELVES

Self-awareness—*Recognizing your emotions as they happen.*

- » Emotional Awareness: Recognizing your emotions and their effect.
- » Accurate self-assessment: Knowing your strengths and limits.
- » Self-confidence: A strong sense of self-worth and capabilities.

Self-regulation—*Using self-awareness to better manage emotions.*

- » Self-control: Keeping disruptive emotions and impulses in check.
- » Trustworthiness: Maintaining standards of honesty and integrity.
- » Conscientiousness: Taking responsibility for personal performance.
- » Adaptability: Flexibility in handling change.
- » Innovation: Being comfortable with novel ideas and approaches.

Motivation—*Understanding the emotional tendencies that guide or facilitate reaching goals.*

- » Achievement drive: Striving to improve or meet a standard of excellence.
- » Commitment: Aligning with the goals of the group or organization.
- » Initiative: Readiness to act on opportunities.
- » Optimism: Persistence in pursuing goals.

Employees who rated supervisors as having high EQ felt more engaged and that their work was more meaningful, according to a 2016 Yale Center for Emotional Intelligence survey.

- » **Empathy**—awareness of others' feelings, needs, and concerns. Empathy is fundamental to building good relationships, though many internal auditors disregard empathy in their effort to maintain objectivity, logic, and a reliance on facts. Mark sees discussion of the audit results strictly as a logical exercise, and he expects the same from Dave. But Dave's emotions are driven by his attachment to the project—a project he perceives as under attack. The disconnect immediately causes a conflict and impedes successful communication.
- » **Social skills**—the art of inducing desirable responses in others.

Mark could have approached the meeting differently had he understood the audit's potential impact on Dave or at least given more thought to the reason for Dave's negative response. He could have instead focused on the shared goals of process improvement and ensuring project success.

EQ AND INTERNAL AUDIT

The story of Mark and Dave provides just one example of how EQ principles can help internal audit work more effectively with clients. Because almost all aspects of internal auditing benefit from improved interpersonal relationships, the impact of enhanced EQ is far-reaching and spans numerous applications.

Interviewing The key to successful interviewing is gaining the interviewee's trust, allowing him or her to feel comfortable sharing information openly and honestly. Applying EQ during interviews begins with understanding any emotions the interviewee may be experiencing—such as fear of saying something wrong, anger at interrupting a daily routine, or apathy about the entire process—and addressing these concerns up front. Auditors should explain the purpose of the interview, as well as what can be expected during the process.

As the interview progresses, the auditor also should be aware of reactions that indicate the interviewee's emotions may be inhibiting free exchange of information. The auditor should address these emotions—not just the words spoken. This can be as simple as pausing the interview to ensure the interviewee is comfortable—in the room, in the situation, and with the approach being used. It also provides an opportunity to reiterate the purpose of the interview and explain how it is intended to benefit all parties. If the interviewee still seems reticent, the auditor needs to determine whether the interviewee has concerns about the process, with the questions, or with something in the work environment. Similarly, internal auditors should consider how their own emotions may be interfering with effective communication, try to bring those emotions under control, and then proceed with a calmer state of mind.

Meetings Many of the EQ principles used during interviews also apply to meetings. Auditors should pay close attention to participants' emotions before the meeting, watch for any escalation of negative emotions, and avoid getting swept up in their own emotions.

Nonetheless, the emotional dynamics of meetings can be more complicated than interviews because

SOCIAL COMPETENCE—HOW WE MANAGE RELATIONSHIPS

Empathy—Awareness of others' feelings, needs, and concerns.

- » Understanding others: Sensing other's feelings and perspectives, and taking an active interest in their concerns.
- » Developing others: Sensing others' development needs and bolstering their abilities.
- » Service orientation: Anticipating, recognizing, and meeting the needs of customers.
- » Leveraging diversity: Cultivating opportunities through different kinds of people.
- » Political awareness: Reading a group's emotional currents and power relationships.

Social Skills—The art of inducing desirable responses in others.

- » Influence: Using effective tactics for persuasion.
- » Communication: Listening openly and sending convincing messages.
- » Conflict management: Negotiating and resolving disagreements.
- » Leadership: Inspiring and guiding individuals and groups.
- » Change catalyst: Initiating or managing change.
- » Building bonds: Nurturing instrumental relationships.
- » Collaboration and cooperation: Working with others toward shared goals.
- » Team capabilities: Creating group synergy in pursuing collective goals.

Adapted from *Working With Emotional Intelligence* by Daniel Goleman.



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

of the number of people involved. The auditor must watch for and balance participants' reactions to ensure no one projects negative emotions that could derail the meeting's objective. At the same time, the emotions of any other auditors in the meeting must be monitored to ensure the discussion remains focused. For these reasons, everyone within the internal audit department should have an understanding of EQ. If the entire team is adept at applying

scope. However, this structure has no bearing on what motivates the readers of the report. Beginning the report with a description of how results will impact the achievement of objectives may align more closely with the client's needs.

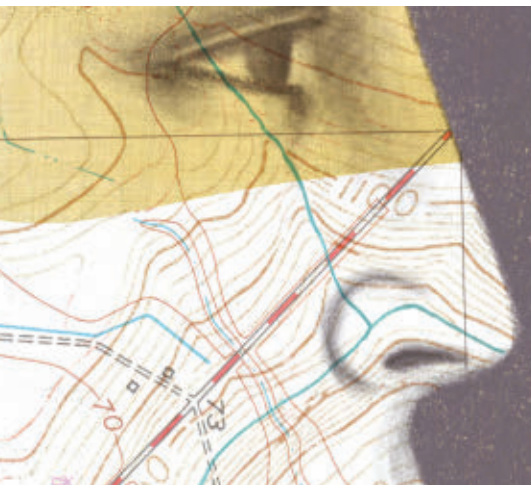
Feedback Just as EQ is important to client interactions, it is equally important to interactions with other internal auditors. One of the more impactful areas is providing feedback. At some point in their career, most practitioners have received review notes that did not make sense, provided no value, or in general caused them to respond negatively. By understanding what caused these reactions, auditors can better determine how to prevent them when giving feedback to other members of the team.

The reviewer must consider that, no matter how well intentioned, any feedback can be construed as criticism. He or she must anticipate and prepare for this reaction by ensuring everyone understands the benefits of the review and by focusing on the facts—describing what needs to be improved—rather than on the personal traits of the individual being reviewed.

Team Dynamics When an audit department understands and practices EQ concepts, the team will be stronger. Team members will have a better understanding of how to work together effectively, with the ability to gauge and adjust their reactions with each other. They can also work in concert to better align their approaches with other departments, helping minimize negative reactions and build better relationships.

Auditors also should consider EQ when hiring. The right questions can help ensure candidates will work well within the department—and within the overall organization. Interviewers should determine not only how much candidates know about EQ, but how well they practice the necessary skills. For example,

When an internal audit department understands and practices EQ concepts, the team will be stronger.



EQ concepts, they can work together to monitor and manage their responses, as well as those of the other attendees.

As with interviews, explaining what to expect before a meeting can benefit all participants. By providing an agenda ahead of time, internal auditors can help ensure meetings run efficiently and smoothly. On a more fundamental level, the agenda can assuage any concerns or fears clients may have about the scheduled discussion.

Reporting Auditors often approach reports as a logical exercise, methodically describing the audit process from background and purpose to final conclusions. However, the concepts of EQ show that readers bring much more than logic to the document. Anticipating potential reactions and crafting each report to mitigate them will help improve report content and establish better communication. Internal audit departments also may want to consider changing their report formats to an approach based on understanding of EQ. For example, most reports begin with the background, purpose, and



VISIT our mobile app + [InternalAuditor.org](#) to watch a video on emotional intelligence.

one of the most commonly asked interview questions is, “What is your greatest weakness?” Generally, people are advised to answer this question by turning a strength into a weakness. But candidates with a high EQ will have already asked themselves this question and will be prepared to describe a true weakness, including how they are overcoming it.

HOW TO IMPROVE EQ

The process of enhancing one’s EQ can be an extensive journey, and it is an important enough topic that all internal auditors should explore available resources (see, for example, “Further Reading,” this page). Some basic steps can help practitioners get started.

First, auditors should look to understand and exert appropriate control over their emotions, always remaining mindful of how their emotions might be affecting interactions with both stakeholders and other auditors. And, as practitioners become more aware of how their reactions impact their work with others, they should determine how to better manage those emotions in ways that help improve relationships.

Beyond this initial step, all interactions should be viewed through the prism of the Emotional Competence Framework. Simple practices can enhance anyone’s EQ. These include giving listeners sincere appreciation, talking in terms of the listener’s interests rather than one’s own, saying “we” instead of “I,” welcoming constructive criticism, and not forcing one’s point of view on others. As internal auditors gain more familiarity with the concepts, they will begin to develop their own effective practices for improvement.

HIGH EQ, BETTER PERFORMANCE

Before recognition of EQ’s importance, attention to emotions in the business world was often frowned upon. In fact, many business people still feel uncomfortable talking about this soft area. But

FURTHER READING

Numerous resources can be found on the basics of EQ and how it applies to business. A web search will yield some of the latest information, though several books, in particular, can provide a starting point for individuals who want to better understand the relevant concepts and improve their EQ.

Emotional Intelligence: Why It Can Matter More Than IQ

Daniel Goleman

This book introduced EQ to the general public. While it does not focus on the business world, it provides an in-depth introduction to the concepts of EQ, including details on the underlying research.

Working With Emotional Intelligence

Daniel Goleman

In this follow-up to his previous book, Goleman discusses and explores EQ as it relates to the business world. It includes numerous real-world examples of EQ done right and wrong.

HBR’s 10 Must Reads on Emotional Intelligence

This collection of articles from various authors represents the best that have appeared in the *Harvard Business Review* on the subject of EQ. The articles include detailed information on how EQ impacts areas such as leadership, teamwork, and feedback.

Emotional Intelligence 2.0

Travis Bradberry and Jean Greaves
Bradberry and Greaves are cofounders of TalentSmart, an organization that provides EQ testing and training. The book provides specific steps to increase one’s EQ as well as access to a free self-test to determine current EQ.


105 Tips for Creating an Emotionally Intelligent Organization

Patrick Merlevede and Gary Vurnum, editors

Various authors provide several short tips for improving EQ within an organization. Focused around seven aspects of organizational improvement, each tip is less than one page and intended to provide simple ideas that can be acted upon immediately.

research consistently shows that star performers possess high EQ. Individuals with superior EQ excel in areas such as communication, conflict resolution, team building, and personnel development, all of which are among the most important soft skills for auditors to possess.

Understanding and practicing EQ competencies can help anyone build better and stronger relationships

with those around them. And those strengthened relationships can play an instrumental role in an internal auditor’s ability to help protect and enhance organizational value. 

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



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.

Implementing a *Shared Services Model*

When consolidating services, internal audit's broad knowledge of the business works to the organization's advantage.

M

any organizations are pursuing sustainable cost reductions via a shared services model. A shared service is a centralized service that was once found in more than one department of the organization such as accounts payable, supply chain, accounts receivable, human resources, and IT. Auditors are increasingly expected to expand their traditional audit services to include consulting expertise around a shared service implementation.

While the benefits of shared services are many, the implementation of a shared services model has potential pitfalls. Though organizations may want to achieve the cost reductions associated with a shared services model, this may

be a high-risk decision unless there is a well-thought-out strategy. Internal auditors can play a key role in that strategy during the implementation phases of a shared services model.

PRE-IMPLEMENTATION

Internal auditors can add value to the organization by providing consulting services before implementation of a shared services model. During the pre-implementation phase, decisions include determination of the business functions best suited for a shared service, technology platforms to improve efficiency of the shared service, and personnel decisions that will align employees with the shared services model. During this phase, management also should be developing

Darrick Fulton
Nandini Parchure

the project charter and metrics for the shared service center. Internal audit can provide insight on various operational, financial, and regulatory risks, and evaluate management internal control design during this stage.

A primary goal for internal audit during this phase is to consult with the business to ensure an effective internal control structure is designed during the implementation. To accomplish this goal, coordination with management should focus on areas management has determined to be best suited for shared services implementation and the various risk factors that can

are approved correctly during product charter development.

IMPLEMENTATION

The challenges management may encounter during a shared services implementation include coordinating various geographic locations, maintaining a good transaction turnaround time, and ensuring quality customer service. Internal audit should focus its efforts on helping management address these challenges. As part of its consulting services, internal audit can work with management to ensure these questions have been addressed adequately or anticipated by management before implementation:

- » Are the decision rights well defined, communicated, and understood?
- » Have policies and procedures been established?
- » Has a project management plan, aligned with the goals of the shared service center, been submitted and approved?
- » Are appropriate internal controls being planned?
- » Will the shared service use the existing system/technology platform, a new system, or both?
- » Have IT solutions such as e-procurement or imaging tools been considered to improve process efficiency?
- » Do employees have the appropriate system access with attention given to segregation of duty concerns?
- » Is the right staff in place with the skills and desire to deliver quality services to customers, drive cost efficiencies, and initiate improvements?
- » Do employees have appropriate training?
- » Has management considered how to ensure a control environment is maintained after the transition?

The internal auditor's knowledge of operational processes can provide insight to management.

negatively impact a successful implementation. Internal auditors with backgrounds in IT, human resources, or accounts payable may be considered particularly helpful in these discussions. IT auditors can be used to ensure IT system decisions are given appropriate due diligence.

Another consideration during the pre-implementation phase is identifying operational redundancies that can be eliminated within the processes. Current industry practices or trends regarding shared service centers also should be considered. For example, traditional financial shared service centers (e.g., accounts payable) versus nontraditional (e.g., corporate communication and legal) can present different challenges. The internal auditor's knowledge of operational processes can provide insight to management in the decision-making process. Auditors also can help ensure the right stakeholders are identified and decisions



- » Have regulatory considerations in different states or countries been evaluated and addressed?
- » Have key performance indicators (KPIs) been determined to evaluate performance and make adjustments accordingly?
- » Have KPIs been organized into effective scorecards? (See “Scorecard Metrics” on this page.)

While providing consulting services, internal auditors should maintain objectivity and independence. Most independence concerns can be removed by ensuring the auditors do not assume management decisions and do not process transactions. However, careful consideration should be given to safeguard compliance with professional standards.

POST-IMPLEMENTATION

Once the shared service center is in operation, auditors can test transactions, monitor service levels, and recommend process improvements through objective reviews of operations. Auditors should review the monitoring and testing of shared service controls as part of continuous monitoring, or compliance, operational, or process-driven audits. Because the shared service is now functioning for the entire organization and the impact can be greater if there is a process breakdown, audits should be conducted promptly. After implementation of the shared services model, auditors should consider these audit procedures:

- » Test IT access to ensure appropriate access and segregation of duties.
- » Test reports (KPIs) to determine data accuracy and completeness.
- » Identify transactions outside established parameters using data analytic tools and techniques.
- » Determine specific regulations by geographic location or industry.

SCORECARD METRICS

Scorecards can alert management of a process or control breakdown and help determine which reports should be used to gather performance metrics. Scorecards can include a variety of key performance indicators, and can be developed in these categories.

Financial

- » Cost savings achieved.
- » Year-over-year unit-cost targets and trends since implementation.
- » Budget vs. actual vs. historical reviews.
- » Fixed vs. variable expenses.
- » Activity-based costing to evaluate the cost effectiveness of specific activities within the shared service center.

Customer or Stakeholder Satisfaction

- » Tracking of information received from customer satisfaction surveys.
- » Number of customer complaints.
- » Feedback from internal stakeholders.

Process Management

- » Productivity measures.
- » Quality metrics.
- » Turnaround trends (e.g., the number of invoices processed per day and per employee).
- » Number of transactions processed in a day, reviewed for trends.
- » Cases touched or issues raised multiple times.
- » Number of transactions in a hold or pending status.

People

- » Employee engagement survey results.
- » Employee retention and attrition rates.

- » Test controls to verify regulatory compliance.
- » Review the reporting process management has established to ensure performance is in line with expectations. Gain an understanding of the actions taken when actual metrics are outside of expectations. Review the scorecards in place to assess and manage performance.
- » Verify the application of policies and procedures to the process, review known control breakdowns and ongoing challenges,



Get the Risk Bundle That Nails It!

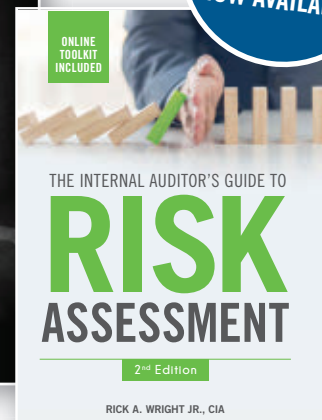
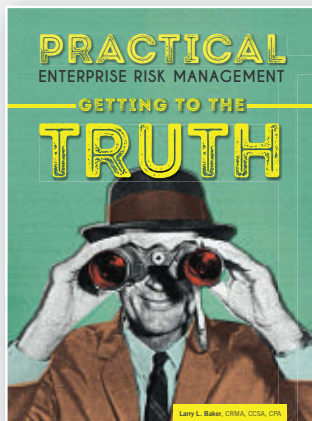
Risk challenges come from every direction. To hit the mark and make sure you're covered from every angle, you must draw from a variety of resources.

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

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

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

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



BUY YOUR BUNDLE TODAY!
Visit www.theiia.org/RiskBundle



Bookstore
Powered by the Internal Audit Foundation

73% of companies report an **increase in productivity** of 5% or higher from a shared services model, according to Deloitte's 2017 Global Shared Services Survey.

and verify that appropriate approval controls have been embedded in the process.

Refer to Standard 1130.A3 regarding the internal audit activity providing assurance services where it previously performed consulting services to ensure independence and objectivity.

UNIQUELY QUALIFIED

In addition to cost savings, a successful shared services implementation can result in important benefits for organizations, including consistent processes and quality standards across the organization and enhanced business process integration following mergers or acquisitions, which can result in improved quality and productivity. The alignment of business services in a global operating structure often

results in better information for management decision-making. A shared services model also allows local business managers to focus more on items of strategic importance, such as business development and improved customer service. On the technology side, system enhancements typically involved in a shared services environment serve to improve the effectiveness of the shared service operation.

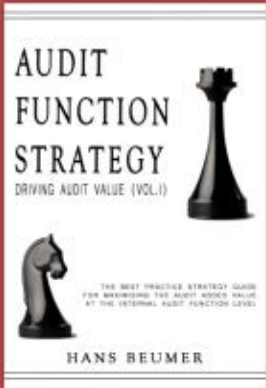
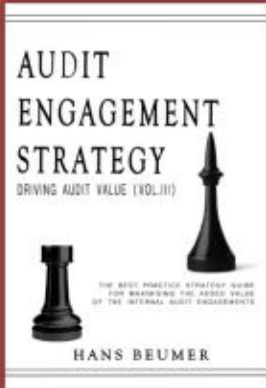
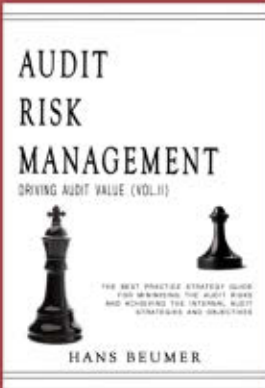
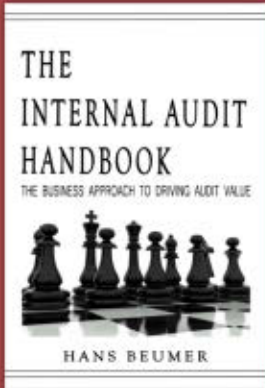
There also are human resource benefits to a shared services model, as the expertise of shared service employees benefit the entire organization, and in-house expertise is developed versus outsourcing for that skill. Challenges with attracting and retaining employees have decreased as companies find innovative ways to make shared services a specific career path.

Because of their knowledge of the business and its related processes, auditors should work with management during the planning and implementation phases of a shared services model. When wearing their consultant hats, internal auditors can add value during the post-implementation phase of the shared service to ensure the service is functioning as intended and significant problems are quickly identified and corrected. Performing consulting activities is part of the Definition of Internal Auditing, and it can be a significant benefit to organizations in the rapidly changing global business environment. [Ia](#)

DARRICK FULTON, CPA, is a senior auditor at Spire Inc. in St. Louis.

NANDINI PARCHURE, CPA, is a senior auditor at Spire Inc.

NEW – INTERNAL AUDIT BEST PRACTICE STRATEGY GUIDES

	+		+		=	
<p>Maximising internal audit added value at the internal audit function level</p> <p>ISBN 9783906861135</p>		<p>Maximising internal audit added value of the internal audit engagements</p> <p>ISBN 9783906861180</p>		<p>Minimising internal audit risks to achieving internal audit strategies and objectives</p> <p>ISBN 9783906861159</p>		<p>The business approach to driving internal audit value on 740 pages</p> <p>ISBN 9783906861203</p>
<p>Available in Print and eBook, at the IIA Bookstore, www.theiia.org/Bookstore or Amazon, Lulu, iBook Store, Barnes Noble, Ingram</p>						

GOVERNANCE



MP.P / SHUTTERSTOCK.COM

Done right, corporate governance audits can generate great value for organizations.

IN VIEW

Doug Watt
Brian Schwartz



Today's business landscape creates some tricky terrain for organizations to navigate. Heightened scrutiny of boards and management, and transformational internal and market forces are the rule, rather than the exception. In this environment, a corporate governance assessment can yield significant value for organizations. Moreover, it enables internal audit to satisfy the requirements of Standard 2110: Governance.

Corporate governance is the system of rules, practices, and processes by which an organization is controlled and directed. It sets the foundation not only for business protection and strategic performance, but also for the confidence of the markets, investors, regulators, and other key stakeholders. Effective corporate governance is a

powerful driver for achieving strategic objectives in dynamic environments while supporting a strong risk culture (see "The Value of Corporate Governance" on page 51).

LAYING THE GROUNDWORK

Determining whether strong corporate governance practices are in place entails taking a hard look at big-ticket issues such as the board's and the executives' roles and practices, how leadership sets and agrees on strategy, how that strategy translates into overall action plans, how those plans are managed, and how progress is measured against goals. Performing this analysis has enormous advantages, but there is a potential catch. This is an assessment of the top of the organization—its board, management,

business strategy, and risk management and compliance functions. The return is high, but so are the risks to internal audit. Planning, execution, and reporting must be aligned to the broad based stakeholder group so internal audit's findings and recommendations are fully supported and acted upon. That makes it imperative that corporate governance audits are well planned and skillfully executed. Internal audit must obtain the necessary buy-in at the highest levels,

Delving into governance audits without the right expertise, timeline, and scope can hurt the internal audit function. Depending on its depth of expertise, internal audit may want to bring in third-party subject-matter specialists to provide additional credibility, experience, and an industry sector perspective that is benchmarked against leading practices. Working closely with outside subject-matter experts also provides an excellent knowledge transfer

its objectives and monitor how it performs.

- » Maintains the integrity of the organization's structure and accountability.
- » Influences the appropriate tone and risk culture.

Risk culture merits special emphasis because it is at the heart of corporate governance. If internal auditors fail to consider the organization's risk culture, they may miss the subtle indicators of ineffective governance. For example, a company may have a well-designed governance structure but ineffective governance because its risk culture discourages managers from escalating risk issues for fear of the consequences.

Finally, the organization needs to decide where it wants to be in the corporate governance maturity model. Does it want to be a leader in one or more areas, or is average sufficient? A corporate governance audit can benchmark where the organization stands on categories ranging from board governance to strategic planning to tone at the top to risk management and corporate compliance. For each of these areas (and more), auditors can chart whether the organization is lagging, average, or leading against peers.

If internal auditors fail to consider risk culture, they may miss the subtle indicators of ineffective governance.

provide excellent communication and project management throughout the audit, and ensure it has the right expertise focused on the review from the start through the final deliverable.

As chief audit executives consider these issues, they should keep in mind the expectations of key stakeholders such as the board, C-suite, and business unit management. Without stakeholder commitment—including making time for interviews, reviewing results, and implementing improvements—the audit can't succeed. By seeking high-level input and perspective early on, internal audit can respond to stakeholder concerns, incorporate their priorities, and ensure the audit goes forward with the appropriate backing from senior management.

It's also important to focus on the organization's external stakeholders such as regulators, shareholders, and external auditors. Once announced, internal audit's decision to undertake a corporate governance audit will generate intense interest. Auditors should prepare for regulator requests to look at their approach and findings.

opportunity that can assist internal audit in future reviews.

GOVERNANCE AND RISK

A look at the corporate governance risk framework is a helpful way to understand the structure for an audit (see "The Corporate Governance Risk Framework" on page 53). Internal auditors should ask several questions about the organization's corporate governance framework. Auditors at highly regulated organizations already may be hearing these questions from regulators. However, any organization would benefit from exploring whether its governance model:

- » Guides strategic direction and day-to-day control.
- » Outlines the rules and procedures for making decisions.
- » Specifies and distributes rights and responsibilities, including decision-making authority, among the organization's various stakeholders.
- » Provides structure and accountability through which the organization can achieve

STRUCTURING THE AUDIT

There is not one ideal way to assess the state of corporate governance. An example of an approach that is well-suited to an organization embarking on this process for the first time is to execute a two-phase assessment comprising an initial advisory phase and an audit phase.

Advisory Phase In the first phase, the goal is to establish a baseline by focusing on the entire governance framework. The assessment relies heavily on interviews with a selection of board members, senior executives, and others in the organization. The questions should focus on a broad range of

27% of internal auditors say their department conducts **extensive reviews** of general governance policies, according to The IIA's Common Body of Knowledge Global Internal Audit Practitioner Survey.

THE VALUE OF CORPORATE GOVERNANCE

Corporate governance has several tangible benefits:

- » **Meeting heightened expectations of regulators and stakeholders.** Faced with unprecedented scrutiny, many boards are challenged to move their organizations forward while meeting the ever-increasing demands of stakeholders and regulators.
- » **Managing the organization's shifting risk profile because of internal and market forces.** Organizations in many industries are striving to transform themselves. Changing business models and expansion into new businesses, services, and products continually reshape an organization's risk profile. Adapting corporate governance to these new realities is an important component of a successful business transformation.
- » **Identifying blind spots that could impede achievement of the organization's strategy.** Without strong corporate governance, organizations may struggle with conflicting objectives or a competing strategy that is diverting resources from a priority project.
- » **Addressing concerns about risk culture.** Without a business strategy, it's difficult – if not impossible – to determine whether the organization is taking appropriate risks. Robust corporate governance can maintain focus on the organization's strategy and how it aligns with its risk culture.
- » **Surveying the organization's lines of defense.** There's a great deal to be gained from looking carefully at the organization's 1) revenue-generating business units and their accountability for the risks they create, 2) risk management teams and the framework they have created for business units, and 3) internal audit function, including internal and board reporting objectives.



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

governance topics, including corporate strategy, board oversight and committee structure, management committee structure, tone at the top and culture, the state of the compliance program, and the state of the risk management program. At the highest level, these interviews should provide a view of their understanding of the organization's governance processes and how those processes are aligned with corporate objectives.

Auditors also should review supporting documentation, such as bylaws, board committee charters, policies, and organizational charts, to create a holistic picture of the organization's culture and processes. They then should analyze information developed through the interviews and document review processes and assess it against a maturity scale. Audit recommendations should assist the organization to ultimately move farther along that scale.

A corporate governance assessment will require the audit team to make qualitative judgments about the design of the governance structure. Internal audit will need to determine how formal the corporate governance

Performing the initial work as an advisory review allows for a freer two-way exchange of ideas.

elements should be compared to leading practices in the industry and at peer companies. Performing the initial work as an advisory review allows for a freer two-way exchange of ideas and observations ahead of the formal audit.

During the advisory phase, internal audit should communicate the results of its interviews and assessment

Featuring

Internal Auditor Blogs

Voices with viewpoints on the profession

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



Chambers on the Profession:

Seasoned
Reflections on
Relevant Issues



From the Mind of Jacka:

Creative Thinking
for Times
of Change



Solutions by Soileau:

Advice for
Daily Audit
Challenges



Points of View by Pelletier:

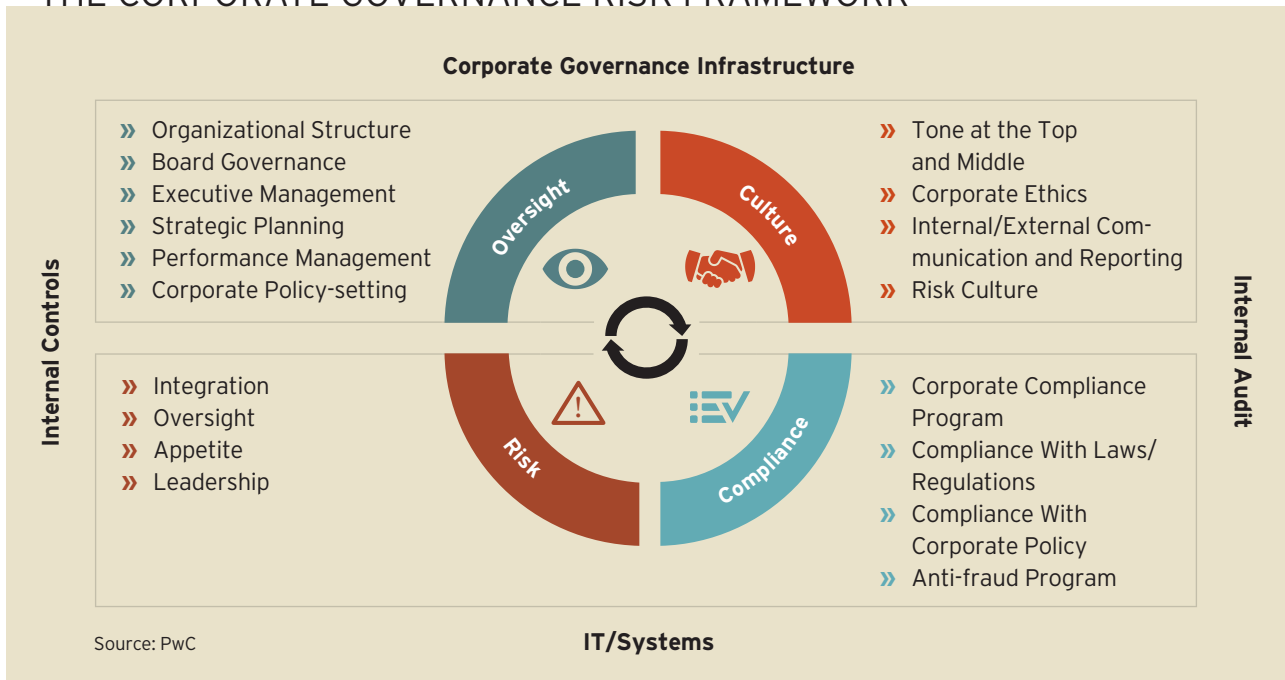
Insights and
Innovations
From an Insider

READ ALL OF OUR BLOGS. Visit InternalAuditor.org.

Ia
INTERNAL AUDITOR

68% of directors say their board made **improvements** in 2017 as a result of its performance assessment, up from 49% in 2016, according to PwC's 2017 Annual Corporate Directors Survey.

THE CORPORATE GOVERNANCE RISK FRAMEWORK



to management as recommendations instead of formal issues. The absence of an opinion positions the internal auditor as a business advisor, which promotes candid discussions and more informed recommendations.

At the end of the advisory phase, suitable time is needed to allow the organization to implement corrective actions in response to recommendations resulting from the first phase. The amount of time depends on the extent of remediation required and often will be more than a year to allow for policies to be developed or enhanced and implemented.

Audit Phase With an established framework in place, the company can conduct a formal audit to assess the effectiveness of governance processes. Here, the scope is narrower and builds on the previous review work. As during the first phase, interviewing board members and executives is a key component.

In-depth testing of key risk areas also is important. Examples of key risk areas include delegation of authority, board and management committee charters, risk appetite, and the compliance testing program. The outcome is an analysis of targeted issues, leading practice recommendations for improvements, and a formal audit opinion.

Internal auditors should keep in mind that they are auditing the leadership of the organization. Presenting corporate governance audit findings to the CEO or board members is the ultimate “seat at the table” for CAEs. They must ensure their facts are thoroughly vetted and benchmarking against leading practices is well supported. Anything short of that could damage internal audit’s credibility.

This two-phase method is just one approach to auditing corporate governance. Organizations with a well-honed governance structure may prefer to start directly with the audit phase. The key

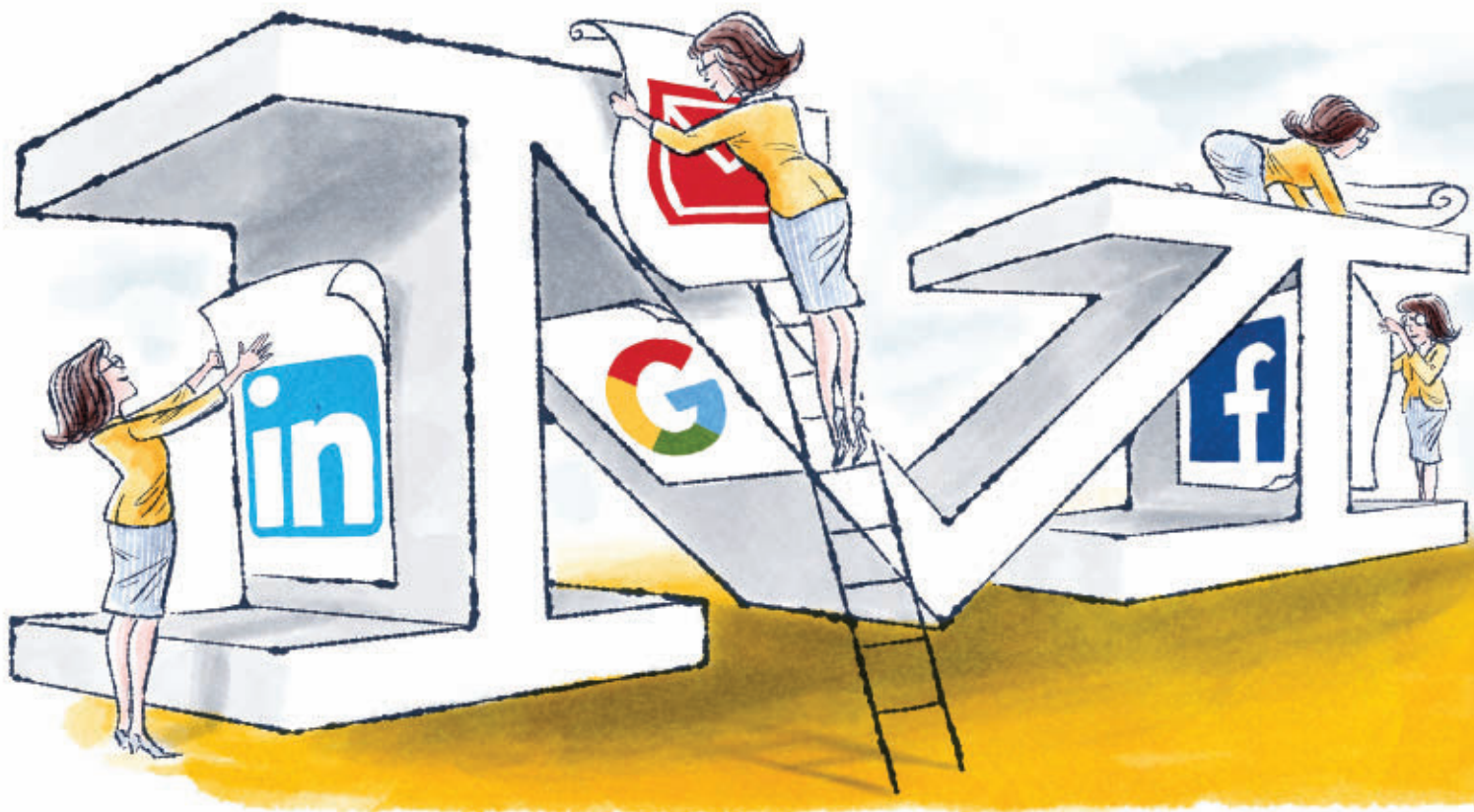
is to tailor an approach for the organization, considering issues such as the maturity of its structures, availability of resources, and leadership and regulatory expectations.

DRIVING CHANGE

The value proposition for a corporate governance assessment is significant. Working closely with the board and senior management, internal auditors have an opportunity to drive change. This is a high-risk, high-reward effort, though. A thoughtful, measured approach and stakeholder buy-in are critical at every stage—from planning through report issuance.

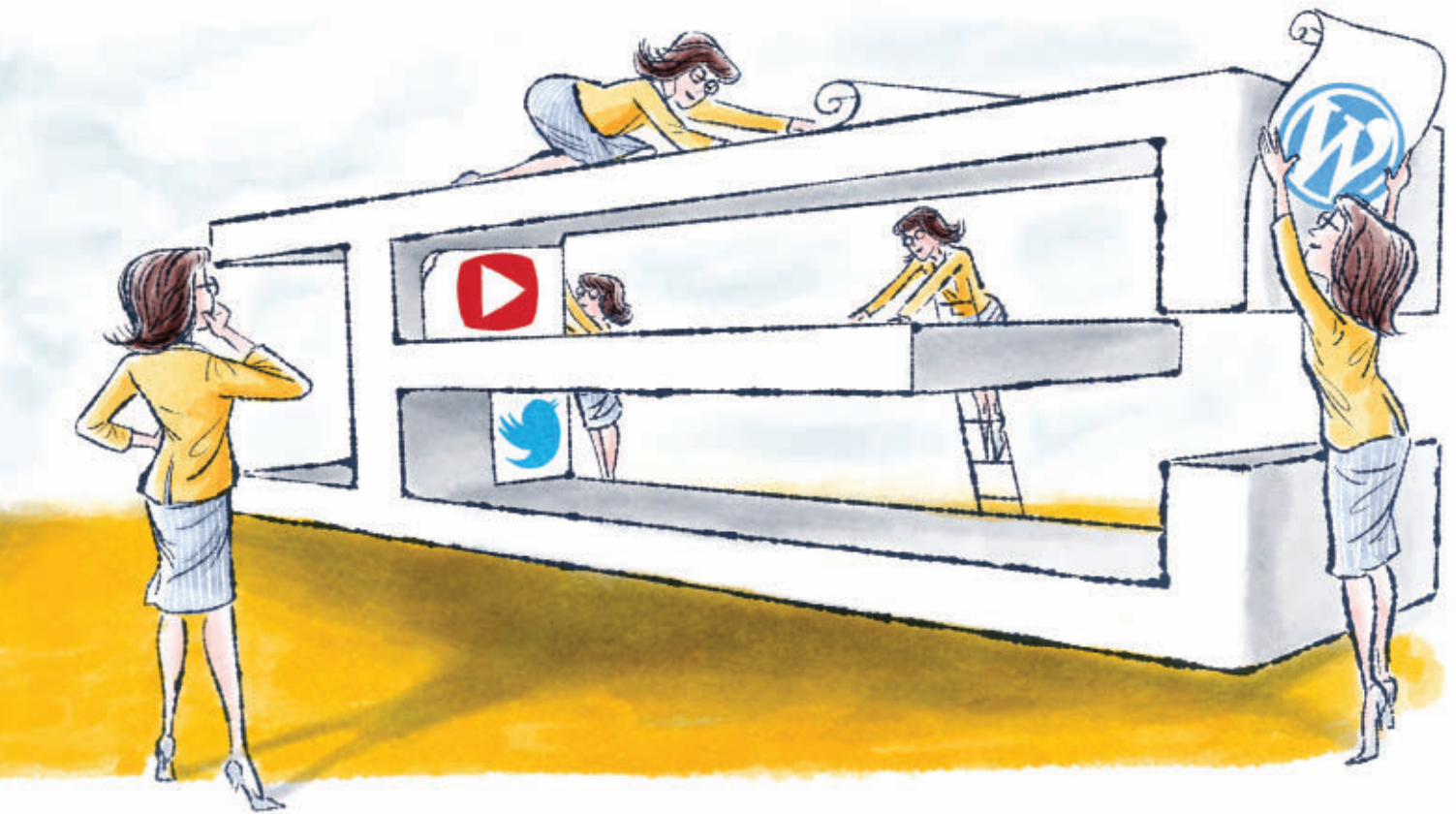
DOUG WATT, CPA, is senior vice president and chief audit executive at Fannie Mae in Washington, D.C.

BRIAN SCHWARTZ, CFSA, CBA, CRMA, CRP, is U.S. Financial Services Internal Audit, Compliance, and Risk Management Solutions leader at PwC in Washington, D.C.



Building a professional identity,
and promoting it effectively,
can be vital to an internal
auditor's career.

your
**PERSONAL
BRAND**



Nancy Haig

Illustration by Edwin Fotheringham

Brands are essential to corporate identity. Successful company branding can make a lasting impression on consumers, solidify market presence, and increase organizational value. At their best, brands establish instant recognition and lifetime loyalty, sometimes representing the organization's greatest asset.

By the same token, personal branding is important for all professionals, and perhaps especially critical for internal auditors. Establishing a brand can enhance an auditor's stature in the organization, as well as increase the perception that he or she can serve as a trusted advisor and provide value. Conversely, practitioners who neglect branding may face significant career adversity, such as finding themselves "on the outs" after delivering bad news to the C-suite or struggling

after a post-merger consolidation of the audit function.

Like an organization's culture, a personal brand exists whether the individual knows it or not. Internal auditors need to intentionally craft their brand—and once established, that brand must be actively managed and maintained.

WHAT IS A PERSONAL BRAND?

More than 20 years ago, management consultant Tom Peters coined the term *personal brand* in a *Fast Company*

PROFESSIONAL ASSOCIATIONS

Joining and actively participating in a professional trade association can help boost one's career, as well as enhance personal branding. Volunteering can include several activities, such as:

- » Participating in a local association chapter.
- » Writing professional certification exam test questions.
- » Writing an article for an industry publication.
- » Speaking at a conference.
- » Creating a video for a trade group website.

article titled, "The Brand Called You." Peters said of personal brand, "Regardless of age, regardless of position, regardless of the business we happen to be in, all of us need to understand the importance of branding. We are CEOs of our own companies: Me Inc. To be in business today, our most important job is to be head marketer for the brand called You."

A more recent notion of personal brand comes from Daron Pressley, a sales and marketing consultant who leads branding workshops. According to Pressley in his *Branding and Brand Management Workshop Reference Guide*, "Success is about the mirror you look into each morning and how you use the reflection you see to shape the life you live. This is personal branding."

Although definitions may vary, *personal brand* almost always refers to someone's authentic personal image—the amalgamation of qualities that make an individual unique. It represents someone's professional presence, encompassing both business skills and personal qualities. Those seeking to define their brand would do well to heed playwright Oscar Wilde's advice: "Be yourself. Everyone else is already taken."

Today, personal brand is often linked to one's social media presence, though every interaction is a branding opportunity—whether in person, through email, or by phone. Failure to treat people with respect, or communicate professionally, can impact personal brand.

WHY IS A PERSONAL BRAND IMPORTANT?

Developing a strong personal brand can benefit an internal auditor's career in many ways. First, it can help a practitioner assess him or herself as a professional and gauge career status. The process requires some homework and self-reflection, which can help reveal

development opportunities the auditor may want to pursue.

Second, an effective personal brand can help an auditor achieve recognition as a well-rounded professional with accomplishments outside of the organization. For example, a brand that encompasses volunteering at a local IIA chapter, participating on a board committee, or making other professional contributions can help auditors stand out as knowledgeable practitioners who advocate for the profession. By doing so, practitioners can increase the likelihood of being perceived as thought leaders, especially when their contributions often consist of offering fresh perspectives.

Third, once their personal brand has been established, internal auditors can more readily determine their career direction and better assess whether they are in the right role, at the right level, and working with the right people. Auditors should then be positioned to make the changes necessary to ensure they are in a truly fulfilling job, resulting in a higher level of performance, engagement, and success through career advancement.

Lastly, the internal auditor, through consistent use of his or her brand, will be seen as a trusted advisor. Others will trust the auditor's reputation, much as they would a product's brand name.

CREATE YOUR BRAND

Creating a personal brand involves building from the inside out. Internal auditors should determine what about their values, personality, knowledge, and experience makes them stand out. Auditors should consider strengths, the benefits they bring to a role, what differentiates them from others, and what they can deliver to the organization.

To better understand how they're perceived, auditors also may want to ask others—colleagues, mentors, friends, or partners—to identify their

95 percent of recruiters view a competitive personal brand as an essential differentiator for attracting the best applicants in today's workplace, according to a 2015 Jobvite survey.

strengths, values, skills, and abilities. If feedback does not align with the auditor's desired image, he or she should take appropriate action to revise personal branding. Practitioners also need to determine their unique professional style, and present that style consistently in all they do. For example, is the auditor's professional style casual and relaxed, sophisticated and polished, focused and analytical, jovial and energetic, or some combination of these qualities?

In a 2013 blog post titled "10 Steps to Building and Managing Your Personal Brand," marketing expert Matthew Royse suggests individuals may want to start with an elevator pitch—a short, concise message that explains who that person is and what makes him or her unique. For internal auditors, the pitch may include whether his or her specialty, or passion, is perhaps information security risks and controls, governance, or quality programs. It can be used for client introductions, job interviews, or social interactions. The elevator pitch also could be adapted for the LinkedIn Summary section of the individual's profile, or on his or her Facebook page, if using the site professionally. Messaging should be continually refined as the auditor's career evolves.

PROMOTE YOUR BRAND

Social media is perhaps the most important means of managing a personal brand online. Professionals can use it to connect with peers, build relationships, and share information that aligns with their brand. After deciding on a personal brand, internal auditors need to determine which social media platforms they'll use to promote themselves.

Some aspects of social media, and specific tools, will better align with brand objectives than others. Auditors should research social media sites to determine which ones are most

compatible with their brand. LinkedIn, for example, provides one of the best platforms for establishing one's reputation as a serious and talented professional, though some may argue that Facebook now also occupies some of



Once established, a brand needs to be monitored to ensure the intended messaging, and the individual's reputation, remain intact.

that space—even though it began as a purely social tool. Twitter also provides a mix of social and professional content, though its unique format and character limit may not be a good fit for individual branding needs.

Internal auditors need to be mindful that their social media content, and overall internet presence, is persistent and readily searched. Therefore, anyone creating a personal brand should remain professional and appropriate at all times. An individual's social media presence reflects his or her values and will often serve as the basis on which that person

is judged. Frank Bucaro, a speaker and ethics advocate, describes on his website how tending to these areas can build one's brand over time. "As trust is proven over and over again, your brand continues to strengthen," he says. "It is actually trust that is branded—trust based on honesty, integrity, ethics, transparency, openness, based on the authoritative use of power!"

MANAGE YOUR BRAND

Once established, a brand needs to be monitored to ensure the intended messaging, and the individual's reputation, remain intact. Auditors can gauge how their presence on social media is being perceived, for example, by reading feedback from blog posts, or responses to comments made on LinkedIn. They can assess whether feedback is positive and whether they need to approach their professional interactions any differently.

Several tools, adapted from Roysse's blog post, can align an individual's online presence with his or her intended branding.

Name Search Internal auditors should search for their name in major search engines, making sure to use variations of their name during the process. The search will help reveal what's been said about the individual online, including any information that may be false or inaccurate. Auditors also may want to find out whether additional information can be found on them in "people databases," such as Intelius and Spokeo. Users can search for themselves on these sites and, for a fee, receive full results. Alternatively, a site like Pipl.com can be used to aggregate these searches.

Upon locating web content that is inconsistent with their brand—or simply inaccurate or false—users can contact the site administrator and ask that their article, comment, photo, or name be removed. Users also can

appeal directly to search engines, such as Google, Yahoo, or Bing, to remove the edited pages. By filling out a simple form, the user can request that the URL be re-indexed. Such requests are not always granted, though instances of confidential, libelous, or copyrighted material will likely have a better chance of success.

When seeking to remove online information, auditors can use tools such as JustDeleteMe or AccountKiller to facilitate the process. JustDeleteMe's and AccountKiller's free tools show users how, and how difficult or easy it

Just as company brands change over time, personal brands also may need to adapt to remain current.

is, to delete unwanted information as well as remove social media accounts that are no longer useful or relevant.

Username Management Ideally, auditors should choose a username consistent with their brand identity and use it as uniformly as possible across platforms. Free tools, including Namecheck.com and Namecheckr.com, can be used to help determine username availability. Users simply type in their desired or current username to find out where the name is registered across social media sites and domains. Auditors can register their desired username on sites they don't currently use, for future application.

Auditors can also use Namecheck.com to create or simplify a personal LinkedIn URL. For example, a profile that appears as linkedin.com/pub/nancyhaig/40/2633/205 could be changed to one that is easier to remember, such as linkedin.com/in/nancyhaig. Users can search via Namecheck.com to determine whether the desired name

is available—if the user's first choice is unavailable, he or she can choose a variation that supports the user's personal brand. The custom LinkedIn URL must contain between five and 30 letters or numbers; it may not include spaces, symbols, or special characters. To change the URL:

1. Login to LinkedIn.
2. Click the "Me" icon at the top of the page.
3. Click "View Profile."
4. On the profile page, click "Edit public profile & URL."
5. Under "Edit public profile

URL," click the pencil icon next to the assigned URL.

6. Type last part of new custom URL in the text box.
7. Click "Save."

Custom Alerts To monitor what others have said about them online, auditors can set up automatic alerts using tools such as Google Alerts or Talkwalker Alerts. To create a Google alert, the user would simply go to google.com/alerts and enter his or her name. To create a Talkwalker alert, the user would visit Talkwalker.com/alerts and, similarly, add his or her name. Both sites provide options such as how often, and in what language(s), the user prefers to be notified. Any instances of those names online trigger an email alert to the user, providing continuous brand monitoring.

Social Management When maintaining a social media presence across multiple platforms, auditors can use a tool to help manage them. Hootsuite, for



VISIT our mobile app + InternalAuditor.org to watch a video on personal branding.

HOW WELL ARE YOU MANAGING YOUR PERSONAL BRAND?

	Yes	No
1 You have a LinkedIn profile.		
2 You believe that being authentic is an important aspect of your personal brand.		
3 You have created a one-minute elevator pitch that describes who you are.		
4 You believe that having integrity is important to your personal brand.		
5 You have created alerts to identify when your name is mentioned on the web.		
6 You are passionate about your career in internal auditing.		
7 You have written an article for an industry publication within the past 12 months.		
8 You have created a video for use on an industry website.		
9 You have uploaded a professional video to YouTube.		
10 You have your own professional website.		



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

SCORING: Give yourself 10 points for every yes and 0 points for every no.

- » If you scored 100, you are in the stratosphere, doing what the most well-known internal audit leaders among us are doing!
- » If you scored between 60 and 90, you are most likely doing a very good job of managing your personal brand!
- » A score between 40 and 50 indicates that you are taking some of the actions that effective internal audit leaders do to manage their brands.
- » If your score was 30 or below, you may want to consider taking additional steps to manage your brand.

example, connects a user's social media accounts and coordinates them through a dashboard interface. The service is free for personal use, for up to three social media profiles, and its features include the ability to monitor conversations, keywords, and phrases across social media. Hootsuite also can be used to schedule and automate the timing of messages, as well as track follower growth to see which content resonates with users.

Website Creation Some internal auditors may want to consider building their own website, particularly if they

decide to start a business or perform consulting work. One helpful site creation resource is Squarespace—an intuitive, out-of-the-box tool available on both desktop and mobile platforms. Squarespace charges users for domain registration and website hosting.

AN ONGOING PROCESS

Just as company brands change over time, personal brands also may need to adapt to remain current. Internal auditors should remember to go back to their trusted colleagues to help refine and refocus their brand, all the while

remaining consistent with their trusted core values. Technology changes also should be monitored to ensure users are using the latest social media tools appropriately to enhance and promote their personal brand. Without deliberate, continual attention to brand building, your brand can turn from highly personalized and effective to one that is defined by others on your behalf.

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

Governance Perspectives

BY MELISSA RYAN EDITED BY MARK BRINKLEY

THE EXTENDED ENTERPRISE

Third-party governance models are a must for today's organizations.

Whether it is referred to as third-party risk, vendor management, supply chain management, or something else, organizations must recognize the risk implications of operating as an extended enterprise. Today's interconnected business models enable companies to leverage partnerships to manage costs and increase competitive advantage. In the extended enterprise, company data and, in many cases, its client or associate data are shared, transferred, processed, or stored by external entities. Very often, this data is among the organization's key information assets. The risk to the entity unknowingly increases when management has not assessed or addressed the potential threats being posed to key assets in this sharing process. These risks may include security protections and associated breach risk, availability standards and associated operational

risk, ownership rights and associated strategic risk, and other key risk points across financial, operational, reputational, and legal areas. Considering these risks and evolving business operations—alongside an increasingly complex regulatory landscape—third-party governance and oversight models are a must-have for organizations.

Gone are the days when an organization's simple inquiry into a new vendor's policies, data security practices, and control structure during the vendor procurement process was considered sufficient. Over time, simple inquiry evolved into a brief, often narrowly focused, evidence or documentation gathering exercise with limited actual review or scrutiny. Fast forward to today when organizations are expected, by stakeholders and regulators, alike, to know, assess, and actively monitor external providers' adherence to defined practices. Internal

audit—and its first and second line counterparts—must determine whether appropriate measures are in place to address third-party risk. This process begins by identifying and understanding two key data points: 1) Who are the organization's vendors and external partners (and their subcontractors or providers)? and 2) What information is being shared with them? Once the landscape and risk profiles are understood, appropriate governance and monitoring also can be established.

Identifying key vendors is the initial step—keeping in mind individual relationships and vendor services structures must be fully understood. Does the organization use an external data center provider? Are there software as a service (SaaS)-based applications used within the organization? Is application development performed by an external provider? Where do external business partners exist

READ MORE ON GOVERNANCE Visit InternalAuditor.org/governance



TO COMMENT on this article,
EMAIL the author at melissa.ryan@theia.org

within key operational business processes? What external entities do the finance, human resources, legal, security, and other corporate teams use to support their functions?

Certain functional areas and systems within the organization can assist in beginning the identification process. Procurement and legal are two functions that should have an understanding of the external partners and associated contracts in place. Review of payables data and vendor master data also can help identify external entities providing services. Discussion with divisional or functional management teams will help validate understanding of the entire third-party landscape, including process dependencies and integration points, as well as the scope of services the vendors provide.

During the identification process a “follow the data” approach should be applied. Internal data governance processes often aid in identifying data components and associated risk. This is the foundation for understanding which data elements to follow in this process. Data that is identified in categories such as “high risk” or with specific regulatory requirements must be traced through its life cycle to all sources. This includes anyone in the vendor process who may handle the data.

During the data tracing process, the consideration of “fourth-party providers” also must be included. Fourth parties (or fifth or beyond) are vendors or subservice providers used by an organization’s direct vendors—extending the risk and governance requirements even further into the supply chain. These can be identified through review of vendor contracts (as they often will specifically state whether services can be subcontracted), but in many cases only are identified during inquiry and discussion with the vendor directly. They all must be assessed as any exposure to risk must be identified and appropriately mitigated.

Along with developing a comprehensive inventory of the vendors providing services across the organization, organizations are well-served by establishing a standard rating or assessment criteria structure to consistently assign a risk classification or other rating to each external business partner. Internal audit can help build or enhance this classification framework based on its understanding of risk assessment principles, as well as its knowledge of business operations and key risk points.

Often, the vendor risk rating or classification structure will include assessment of data being shared, vendor operations, potential customer impact, regulatory considerations, and level of dependency on the vendor for ongoing operations (e.g., system availability or other operational requirements). These categories should be assigned quantifiable metrics where possible, based on risk thresholds established

by the organization. Leveraging this standard classification structure, critical vendors can be identified and the assessment process structured in a prioritized fashion, aligning risk with associated review frequency and depth.

While this article focuses specifically on recommendations to be included in the vendor assessment process, a full vendor management program includes the entire life-cycle process for managing vendor relationships—from planning and selection to ongoing monitoring. Specific design of the vendor assessment process and approach must be aligned with organizational requirements; however, certain focus areas are appropriate for most companies. Common elements may include:

- Information Security—technical configurations, security architecture, access management, monitoring, and incident response.
- Physical Security—facility access, security monitoring, and document control measures.
- Policies and Programs—program and governance models, policies and standards, and reporting structures.
- Human Resources—background checks/verifications and associate training programs.
- Availability—system maintenance and monitoring process, support and operational oversight, and system change processes.
- Business Continuity—disaster recovery and business resumption plans.
- Regulatory Compliance—key requirements may apply to specific data types or industries; the Health Insurance Portability and Accountability Act and General Data Protection Regulation are examples of regulations including specific requirements in regard to third parties.
- Vendor Management—extension of requirements to subservice providers and associated monitoring.

During the vendor review process, it is likely that gaps will be noted between expectations or obligations and actual practices. Effective risk management for third parties also includes ongoing monitoring of vendor response to concerns to ensure they are appropriately addressed.

Implementation and operation of a third-party risk management program is not a small undertaking. However, when considering the business risk associated with vendors and operating with an extended enterprise model, the opportunity for reducing risk and potentially better leveraging vendor partnerships clearly demonstrates the necessity and value of the effort. A measured and phased approach will address the most significant risks as the program matures over time. [la](#)

MELISSA RYAN, CRMA, CISA, leads risk, compliance, and security services at *Asureti in Lenexa, Kan.*



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.



BY J. MICHAEL JACKA

THE PASSCODE IS ... 312

Do you see control issues everywhere? How you respond to them may speak to your expertise as a practitioner.

Recently, I facilitated an internal audit seminar where something unusual occurred. The restrooms at the facility were locked, requiring a code for access. And while this type of security can be found in many commercial buildings, other factors raised questions about the practice.

The event coordinator gave the restroom code to seminar facilitators to share with participants. Someone also had written it on the whiteboard of each room. Moreover, the code appeared on flip charts that pointed the direction to the restrooms, as well on the doors of the restrooms themselves.

Seminar participants started to discuss the situation. The room full of auditors instantly pointed out that displaying the code in so many places represented an obvious breakdown in controls. Some of them compared it to writing a login password on a sticky note and then attaching it to one's computer.

But a couple of attendees took the analysis a little further. They asked the deeper question—the one


that any auditor using critical thinking skills should ask: What was the risk of everyone knowing the code? And as the discussion continued, someone asked another, perhaps more important question: How big was the risk that unauthorized individuals would enter the sanctum sanctorum of the 9th floor restroom when the building had guards on duty to ensure only authorized individuals could gain access in the first place?

What kind of auditor are you? Do you go ballistic when you see a circumvented control? Do you accept the control as is, assuming that, because it existed in the first place, it should continue to exist? Or do you look at a control circumvention and ask why the control existed in the first place and why it continues to exist? Or do you ask even deeper questions about risks, how they have changed, and how people are reacting to them?

A good auditor identifies a control breakdown and determines how to get it working again. A better auditor questions whether the control needed to exist in the first place. But the best

auditor, the auditor who is providing real value to the organization, doesn't put all the focus on the existing process and controls. The best auditor looks at the risks with fresh eyes to better understand exactly what is at risk, how people's actions impact those risks, and how the organization can most effectively respond.

Allow me to go out on a most dangerous limb here and disclose that the code to enter the men's room was 312. And now, security is compromised and disaster may rain down upon us because a control has been circumvented. Of course, to the best of my knowledge, no disaster befell us during the seminar.

What is the worst that can happen when a control is circumvented? And why am I supposed to care about the control in the first place? Those are the questions far too many auditors forget to ask. 

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

PROVIDING INSIGHT

CAEs can take certain steps to ensure they are giving the audit committee what it needs.



SHARON LINDSTROM,
Managing Director,
Protiviti



DAWNELLA JOHNSON, Global
Leader, Internal Audit,
Crowe Horwath

What information does the audit committee want from the CAE?

LINDSTROM First and foremost, the audit committee is looking for information, not data! CAEs should think about the top three to five “takeaways” they would like their directors to get from the audit committee meetings. The CAE also should ask the committee what its area of focus is, so the CAE can avoid guessing and instead concentrate on building a good relationship with the members. Potential areas of audit committee interest include: risk assessment results and trends; internal audit plan coverage and progress; audit results and trends; and remediation status and trends. I purposely repeat “trends,” because this is internal audit’s opportunity to provide information, not just data, by connecting the dots. An audit committee mantra may well be, “Tell me what I don’t already know.”

JOHNSON Questions audit committee members want answered include: What’s the state of the union for the organization in light of our charge as audit committee? What’s going well? What’s not? Why? Are there any concerns we haven’t asked about? If the organization is experiencing significant or unexpected change, what is internal audit’s role in understanding the changing risks and how they’re being managed? What should we be thinking about next? What are the issues the CAE is most focused on?

How do audit committees want that information presented?

JOHNSON Different committees want different levels of detail. Some are very detail oriented, while others are comfortable with a summarized reporting approach. The CAE should have an open dialogue with the audit committee and tailor presentations to the members.

LINDSTROM CAEs can make the audit committee’s risk-oversight role easier with their presentation format. The CAE should start by considering the audit committee’s expectations, its communication style, and the frequency of its meetings. Does it prefer a pre-read or a presentation? How much time has been allotted to the CAE on the agenda? Audit committee presentation materials should be visually appealing—verbiage or data-intensive presentations can lose the audience. Content should report on results and trends, not activities. Internal audit can effectively communicate department performance through the use of dashboards, metrics, and benchmarking.

What don’t audit committees want to see from the CAE?

LINDSTROM Committees don’t want to see an audit plan that is not aligned, or relevant, to the organization’s

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



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

business objectives, strategy, and risks. From an audit execution standpoint, they also don't want to see a lack of context for the severity of identified issues—the “so what” of findings—or recommendations that are not actionable.

JOHNSON A few things: lack of strategic focus, timidity in making tough calls, excessive detail without a clear message, and any sign that management is overriding or unnecessarily managing the CAE.

How should CAEs prepare for audit committee meetings?

JOHNSON CAEs should begin with the end in mind. They should think about the messages each member should walk away knowing. This can help the CAE prepare and help prioritize how the meeting is structured and how materials are organized. The CAE can make sure the key messages or learnings are clearly identified in materials or highlighted during the discussion time. The CAE also should spend time with the audit committee chair before meetings. The CAE has a chance to hear questions or perspective from the chair, allowing the CAE to better understand and address questions from a board member's perspective based on other committees or board meeting discussions. Advance conversation can help

The chair can let the CAE know what's working or what needs to be adjusted to meet the audit committee's needs.

the chair prioritize the agenda more effectively and provide the chair with better insight to manage meeting time with members. Advance time is critical when there is a very dense agenda, or when there may be controversial or tough messages to deliver—for example, repeated poor audit results or lack of business line focus on open internal audit issue resolution.

LINDSTROM The CAE should review the agenda with the audit committee chair before the meeting. For each topic, the CAE should determine the key points he or she wants to communicate instead of simply reading the slides. Also, executive sessions are standard operating procedures, so the CAE should prepare by considering what questions are likely to arise from members, and what “asks” internal audit has of the audit committee, if any.

What makes CAEs indispensable to audit committees?

LINDSTROM “Indispensable” is a measure of what's valued by the audit committee. When I think of the auditor of the future, there are so many ways the CAE can create value

for the audit committee and the organization. Think more strategically when analyzing risk and framing audit plans. Provide early warning signs of emerging risk. Broaden focus on operations, compliance, and nonfinancial reporting, and advise on improving and streamlining compliance management. Strengthen lines of defense that make risk management work. Improve information for decision-making across the organization. Watch for signs of a deteriorating risk culture. Expand the emphasis on assurance through effective communication. Collaborate more effectively with other independent functions. Leverage technology-enabled auditing. Improve the control structure, including use of automated controls. And, remain vigilant with respect to fraud.

JOHNSON The CAE should be indispensable to each audit committee member. There are four elements of the indispensable CAE. First, business acumen. Audit committee members want a high degree of confidence in the CAE's knowledge of the organization and the industry in which it operates. This includes understanding the applicable regulatory environment. Second is vision. Audit committee members want to know the CAE will use that business knowledge to look at the organization and sift through noise to identify the important issues. Third is communication. When necessary, audit committee members want a CAE who can deliver a tough message to management with courage and credibility. Finally, transparency. Audit committee members want transparency from the CAE in their interactions. The previous elements are far less valuable if the audit committee isn't getting direct insights from the CAE.

Why is it important for the CAE to develop a good relationship with the audit committee chair?

JOHNSON The chair can let the CAE know what's working or what needs to be adjusted to meet the committee's needs. The chair also can be a powerful ally if the CAE needs board-level support in the event of disagreements over identified results.

LINDSTROM The CAE's direct reporting line is to the audit committee, so a clear and open line of communication builds a good relationship and helps support an independent and objective function. The committee chair can be an excellent sounding-board as well as an advocate. This relationship can be built through standing meetings in between committee meetings, such as a monthly 30-minute check-point. Also, consider periodic meetings between the chair and the internal audit team, even over breakfast or lunch, to engage both sides more fully. [la](#)



Mobile



Webinars



Online



Specialty
Audit Centers

Ia
INTERNAL AUDITING
Print



Foundation
Partnerships



Conferences

ENGAGE AND CONNECT GLOBALLY

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

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

www.theiia.org/advertise



 The Institute of
Internal Auditors

IIA Calendar



IIA CONFERENCES

www.theiia.org/conferences

MARCH 12-14

General Audit Management Conference
Aria Resort & Casino
Las Vegas

MARCH 14

Women in Internal Audit Leadership Forum
Aria Resort & Casino
Las Vegas

MARCH 15

Environmental, Health & Safety Exchange
Aria Resort & Casino
Las Vegas

MAY 6-9

International Conference
Dubai World Trade Centre
Dubai, UAE

AUG. 13-15

Governance, Risk & Control Conference
Omni Hotel
Nashville

OCT. 1-2

Financial Services Exchange
Renaissance Downtown
Washington, D.C.

OCT. 2-3

Environmental, Health & Safety Exchange
Renaissance Downtown
Washington, D.C.

OCT. 3

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

OCT. 22-24

All Star Conference
Aria Resort & Casino
Las Vegas

OCT. 24-25

Gaming & Hospitality Conference
Aria Resort & Casino
Las Vegas

IIA TRAINING
www.theiia.org/training

FEB. 13-16

Various Courses
Phoenix

FEB. 13-22

Cybersecurity Auditing in an Unsecure World
Online

FEB. 19-22

Statistical Sampling for Internal Auditors
Online

FEB. 19-28

Fundamentals of IT Auditing
Online

FEB. 26-MARCH 1

Vision University
Orlando

FEB. 27

Fundamentals of Internal Auditing
Online

MARCH 5-14

Audit Report Writing
Online

MARCH 5-30

CIA Learning System Comprehensive Instructor-led Course – Part 3
Online

MARCH 6-9

Various Courses
San Francisco

MARCH 13-15

IT General Controls
Online

MARCH 20-23

Various Courses
Boston

MARCH 21-22

Data Analysis for Internal Auditors
Online

MARCH 26-28

Succession Planning: Leveraging and Influencing Millennials and Other Generations
Online

APRIL 3-6

Various Courses
Orlando

APRIL 3-12

Assessing Risk: Ensuring Internal Audit's Value
Online

APRIL 3-26

CIA Learning System Comprehensive Instructor-led Course – Part 2
Online



BY EVA SWEET

THE NEED FOR INTEGRATION

Internal audit functions should adopt a holistic approach to engagements.

In an era when IT is embedded in almost every process, trying to audit operational, financial, and technology controls independently is not an efficient use of resources. Beyond the redundancy of effort, it results in fractured reporting to both the board and senior management. Yet many practitioners continue to use this fragmented approach, despite its numerous disadvantages. To add value and improve the organization's operations—as mandated by The IIA's Definition of Internal Auditing—audit functions should instead adopt an integrated audit approach.

Integrated auditing, as described in an IIA Practice Guide, refers to a holistic approach to internal audit engagement planning and execution that helps ensure all aspects impacting the quality or efficiency of a process are considered. The approach often requires auditors with different backgrounds and areas of expertise, at least during the planning phase, to identify all the risks and exposures that should be part of the audit engagement, including operational, financial,

environmental, technological, and regulatory concerns.

Adopting an integrated audit approach focuses the chief audit executive (CAE) on developing auditors who can plan and perform engagements that consider any activity with the potential to prevent the achievement of organizational objectives. These integrated practitioners can provide an end-to-end understanding that includes policies, procedures, inputs, people, technology, outputs, environmental impacts, regulatory requirements, and more importantly their connection to organizational goals.

Integrated auditors, though, should not be expected to possess expertise in every area. In fact, part of being an effective integrated auditor involves knowing when to call the experts and ask for help. However, integrated auditors should be expected to possess the core competencies needed to plan and perform an internal audit, and to be proficient in applying the International Professional Practices Framework's Mandatory Guidance.

They also should have a deep understanding of

the organization, including its core business and strategic goals, policies and culture, and technology (information and operational). Moreover, they should be well-versed in industry-specific issues, such as those pertaining to geographic location or the market in which the organization operates.

Integrated auditing is a winning proposition for the internal audit activity, individual auditors, and the organization. Integrated audits are more effective because they simultaneously assess financial, operational, and IT risk and controls, and they produce more timely recommendations to improve risk management, operational, and governance controls. The approach may help discover deficiencies that could go unnoticed when performing individual audits, and it can increase internal audit's relevance by providing a more comprehensive view of organizational risk. [la](#)

EVA SWEET, CISA, CISM, is director, IT and public sector standards and guidance, at The IIA.

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

Navigating the Complexities of Corporate Culture

Internal Auditing Around the World, *Volume XIII*

Culture audits are an opportunity for auditors to talk to employees, managers, customers and vendors, and report on whether the company is living its values, or whether they are hollow. Read more from 15 audit leaders featured in this publication.



Download a copy at protiviti.com/iaworld.

start strong.
STAY SMART.



Save Up to \$680 While Pursuing Your CIA in 2018

Earning the Certified Internal Auditor® (CIA®) credential not only proves your competence and credibility, it can earn you respect, promotions, and \$38k more annually.*

Need more incentive? Take advantage of the members-only savings of \$580 on your CIA application, exam registration, and CPE reporting,** plus \$100 off CIA Learning System® exam prep tools. There's never been a better time to get prepped and certified with The IIA.

Visit www.theiia.org/StaySmartCIA to learn more.

*According to The IIA's 2017 Internal Audit Compensation Study (based on U.S. responses).
**CIA designation savings vary.