

Ia

INTERNAL AUDITOR

OCTOBER 2015

INTERNALAUDITOR.ORG

Quality Assurance and
Improvement at Fannie Mae

Budgeting for Data Analytics

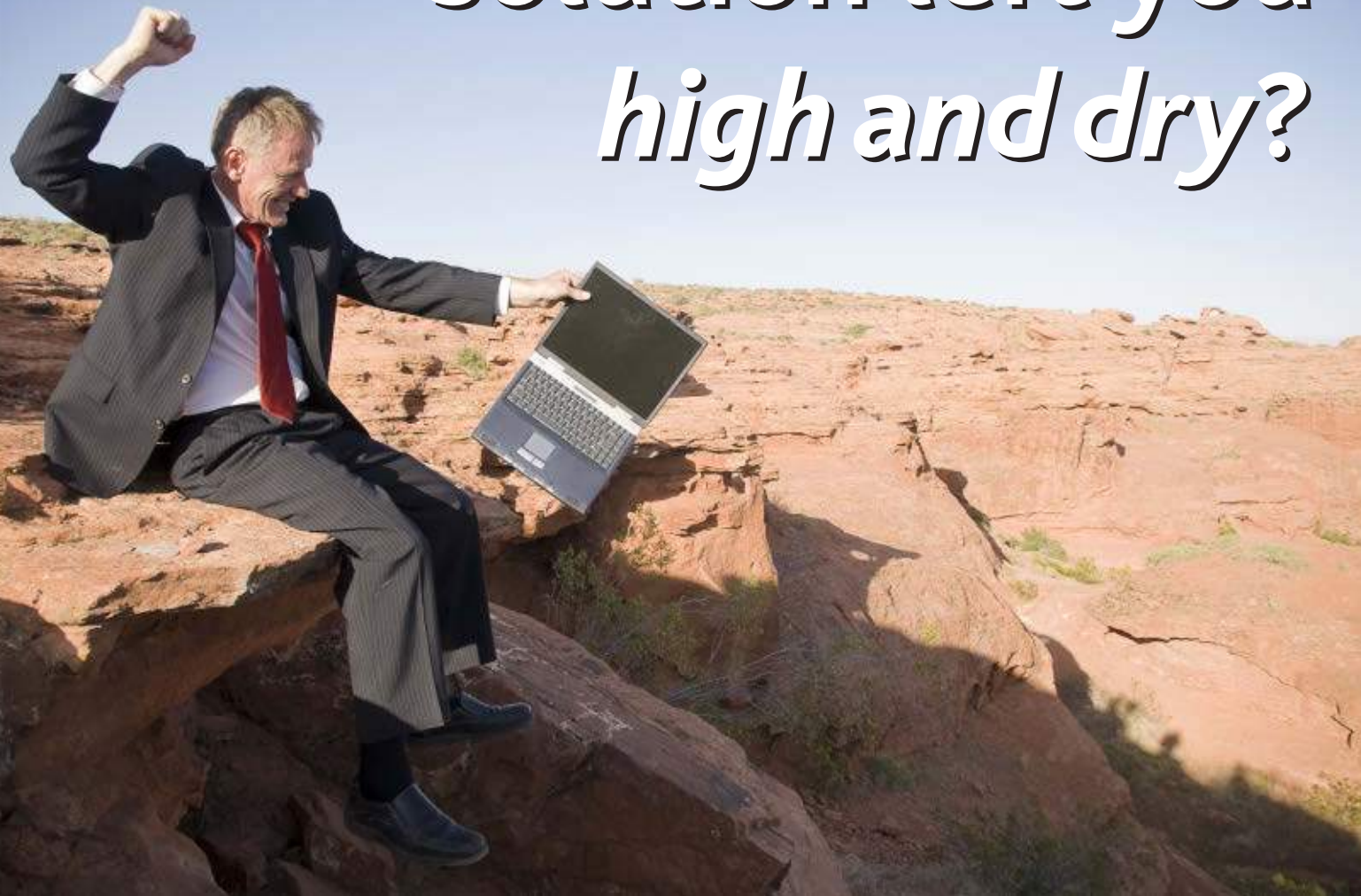
Citigroup's Internal Audit
Foundation Academy

Assessing the Organization's
Moral Landscape

THREE LINES OF DEFENSE

Today's complex businesses require a streamlined way to
organize the many facets of risk management and control.

Has your audit solution left you *high and dry?*



Upgrade to TeamMate by October 31, 2015 and receive **free implementation services, one free year of TeamMate use, or free TeamCloud setup.**

** Limitations apply*

Learn more at
www.TeamMateSolutions.com/RescueMe

Accelerate Your Audit Using Analytic Intelligence



1 1 2 0 1 5

Only With IDEA Version 10

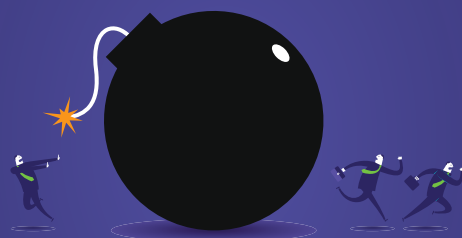
Analytic Intelligence

Backed by 25 years of audit expertise, Analytic Intelligence helps auditors find the starting point in their data. With one click, identify the areas of interest that deserve your investigation.



Find Out How

1-800-265-4332 Ext 2800 | salesidea@caseware.com



Let's stay out of the headlines

Are you tasked with safeguarding your organization? Ineffective and inept internal investigations can be very costly to your bottom line AND reputation.

ACL's comprehensive compliance platform reduces the burden of compliance with a data-driven approach to managing end-to-end compliance processes. Streamline and strengthen your compliance program for regulations such as SOX, FCPA, OFAC, or industry requirements like HIPAA, PCI DDS, Dodd Frank, OMB A-123, AML, or internal governance areas like ITGC, ISO, COBIT, self-assessment and policy certification and attestation.

ACL's Compliance Management Solution helps you:

- Reduce the burden of compliance workload
- Map regulatory requirements to your control framework
- Validate internal controls effectiveness
- Prevent reputation damage and fines
- Streamline policy attestation
- Identify, remediate and track issues



Visit acl.com/Compliance-Management to learn more about taking a centralized approach to compliance management.



FEATURES

26 COVER Defense in Depth Organizations that have adopted the three lines model see collaborative opportunities to address risk. **BY JANE SEAGO**

33 The Value of QAIP Fannie Mae's quality program demonstrates the effectiveness of its internal audit operations in meeting stakeholder expectations.

BY MARGARET ULVI

38 A Strong Foundation Citi Internal Audit undertook an ambitious project to transform its training and development program, enhance consistency, and better meet stakeholder needs.

BY MARK CARAWAN

45 Budgeting for Analytics Using a systematic, sustainable mechanism to determine level of effort can help auditors develop a reliable budget for analytics work.

BY RIGOBERT PINGA PINGA

51 Preserving the Organization's Moral Landscape By assessing integrity and ethics safeguards, internal

audit can help the organization protect against fraud and other wrongdoing.

BY BRUCE TURNER

56 The Effective CAE

Adaptable CAEs who look to make changes in how internal audit addresses critical risks are the biggest benefit to stakeholders.

BY NORMAN MARKS



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

HEADACHES WITH YOUR DATA ANALYTICS PROGRAM?

STRUGGLING TO
GET STARTED

GETTING LOST
IN THE DATA

LACKING THE
RIGHT SKILLS

NOT CREATING
VALUE

OVERWHELMED
BY DIRTY DATA

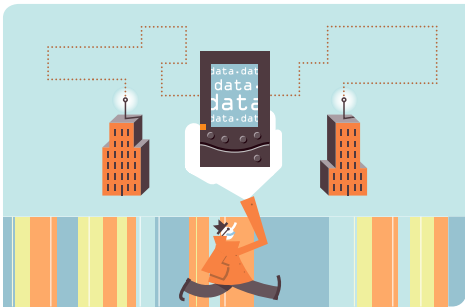
Co-source with us and overcome your hurdles. Our latest whitepaper, "**5 Common Pitfalls of Data Analytics**," provides tips for overcoming common challenges in data analytics.

***Click here** to download the free whitepaper.*



sunera.com | 813.402.1208 | info@sunera.com

DEPARTMENTS



- 7 **Editor's Note**
- 9 **Reader Feedback**

PRACTICES

- 13 **Update** Sharing data across industries aids fraud prevention; government professionals doubt ESI accuracy; and cybersecurity is now a business risk.
- 17 **Back to Basics** Corrected audit deficiencies reinforce a strong control environment.
- 20 **IT Audit** Internal auditors can help thwart social engineering efforts.
- 23 **Fraud Findings** A company suffers under an inattentive board and a crooked CEO.

INSIGHTS

- 65 **Governance Perspectives** Big data presents organizations with both risk and opportunity.
- 69 **The Mind of Jacka** Audit training should go beyond the requisite 40 hours.
- 70 **Eye on Business** Companies need to take a balanced, integrated approach to GRC.
- 72 **In My Opinion** The challenge to change negative perceptions and add value continues.

ONLINE InternalAuditor.org



- The Transformation Journey** When assessing a transformation program, internal auditors should consider five key criteria in their analysis.
- Preparation for a Data Breach** Author James Reinhard maps out how internal audit can establish an audit program based on the U.S. Justice Department's recent cybersecurity guidance.

- Successful Audit Leadership** Watch three experienced members of the National Association of Corporate Directors discuss the skills audit leaders need to succeed in today's organizations.
- The Light Paychecks** Art Stewart weighs in on the case of an Australian convenience store chain that is accused of not paying employees for the time they worked.



TeamMate® ecosystem

Only TeamMate offers the right balance of solutions that includes the industry's leading audit management system, an innovative controls management platform and powerful data analytics. Use them individually or in combination to achieve harmony in your world.

AUDIT

TeamMate AM is an end-to-end audit management system designed to help auditors and department leadership manage all aspects of the audit process. TeamMate streamlines the processes of risk assessment, scheduling, time tracking, work paper documentation, issue identification and tracking, and reporting, giving you more time to focus on true value-added elements of your audit work.



ANALYTICS

TeamMate Analytics includes more than 150 audit tools and runs on top of Excel, allowing auditors to easily perform powerful data analysis and deliver significant value without the need for extensive training. TeamMate Analytics is a powerful standalone solution for any auditor, and gives you the ability to greatly extend the application of data analysis in your audits.



CONTROLS

Managing the numerous and complex regulations and control standards now in place around the world can be a daunting task. Organizations still struggle to find the right solution to manage their controls and address compliance with mandates such as COSO 2013, Sarbanes-Oxley, COBIT, and others. TeamMate CM's streamlined and user-friendly design eliminates the pain of dealing with overly-complex systems or a jumble of spreadsheets.



Learn more at www.TeamMateSolutions.com



Wolters Kluwer



Copyright © 2015 Wolters Kluwer Financial Services, Inc. 4228



THREE LINES, ONE OBJECTIVE

In 2013, The IIA issued The Three Lines of Defense in Effective Risk Management and Control Position Paper to address the number and complexity of potential risks in today's businesses. The paper detailed a streamlined approach to risk management and control built on three layers—operational management, risk management and compliance functions, and internal audit.

Today, the Three Lines of Defense model is used throughout the world. According to a recent Global Internal Audit Common Body of Knowledge (CBOOK) report from The IIA Research Foundation, 55 percent of respondents from publicly traded organizations, 43 percent from the public sector, 41 percent from not-for-profit organizations, and 40 percent of respondents from privately held companies (all excluding the financial sector) around the globe say they are using the model.

As might be expected because of the intense regulatory oversight of financial services, the financial sector is by far the biggest user of the model, with 78 percent of financial services respondents saying their company uses the model with internal audit as the third line of defense. However, an additional 3 percent of respondents in this industry report internal audit is considered the second line of defense, and 10 percent say the distinction between the second and third lines is unclear.

According to the CBOOK report, A Global View of Financial Services Auditing, "internal auditors in financial institutions are challenged with finding ways to effectively implement this model in a way that works for their organization." In some small and midsize organizations, the lines between the second and third lines of defense can become blurred and the roles blended.

As chief internal audit *and* risk officer with Community Trust Bank in Pikeville, Ky., Steve Jameson knows the blurring lines challenge well. "Independence is managed by established safeguards that are documented and reviewed annually with both the audit committee and the board, and both bodies formally approve this framework and my role," he tells author Jane Seago in "Defense in Depth" (page 26). Jameson is a co-author of the financial services auditing report.

As Seago explains, the Three Lines of Defense model's structure is specifically defined; however, it is still flexible, and it is adaptable to support organizations of various sizes, structures, and complexity. "Ultimately, regardless of how the model is implemented, the key is ensuring that all functions are operating in concert to achieve organizational objectives, avoiding gaps in coverage and duplication of effort," she tells readers. In her article, Seago defines the model in detail and looks at the many ways it is being used in practice.

@AMillage on Twitter



EY

Building a better
working world

Can you see what's coming?

Change is inevitable. And it can happen in the blink of an eye. EY's Internal Audit Services can work with you to prepare for what you can see ... and what you can't. Our insights and innovative mindset can help you make the most of your opportunities with the least amount of risk.

To find out more, visit ey.com.audit.

Reader Forum

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.



Dialogue on Data Analytics

I'd like to thank David Coderre for sharing his insights regarding the implementation and use of data analytics in internal auditing.

The internal audit department I work in is in the infancy stages of incorporating data analytics in our audit work. I have been asked to think of areas or opportunities where data analytics could be used. After reading his article, I feel prepared to discuss my ideas with our audit management team and will be able to suggest who the key contacts would be to help bring these ideas to fruition.

MELANIE THOMAS comments on David Coderre's article, "Gauge Your Analytics" (August 2015).

I read and enjoyed David Coderre's article on data analytics. I couldn't agree more with most of the points raised, and, in particular, about the business knowledge necessary for the people identifying potential areas to investigate and the processes and analysis required prior to digging into the data.

I work primarily in the area of accounting forensics and data analytics as it relates to investigations and disputes. The skills needed for analytics, as Coderre points out in the article, are spot on with my work, as well—coupled with the quick learning required on each matter to understand the underlying core of the investigation and dispute—as it relates to the data available.

MARTIN STACKS comments on David Coderre's article, "Gauge Your Analytics" (August 2015).

Data analytics has indeed moved from optional to required; however, the practice of having single-point-of-contact champions and setting up separate analytics functions limits the entire internal audit department. Professional data analysis tools better equip every auditor

on every audit, making them better positioned to understand decisions made from available data. Putting technology within reach of every auditor improves efficiency and effectiveness, yields high returns, improves communication across departments, and benefits and strengthens the organization as a whole. Why would anyone want to limit those benefits to just a select few?

DONALD SPARKS comments on David Coderre's "Gauge Your Analytics" (August 2015).

Author Response: *I agree and strongly encourage all auditors to develop their analytics capabilities. However, analysis is more than using audit software. It requires identifying, accessing, verifying, and cleansing the data before being able to analyze it. A sustainable data analytics capability, particularly where one does not currently exist, is best served by having responsibility for the development of the analytics capability assigned to a person or group. Then, as the article states, "As the audit function moves along the data analytics maturity curve, audit teams can take more responsibility for data analysis,*

Ia

INTERNAL AUDITOR

OCTOBER 2015
VOLUME LXXII:V

EDITOR IN CHIEF

Anne Millage

MANAGING EDITOR

David Salierno

ASSOCIATE MANAGING EDITOR

Tim McCollum

SENIOR EDITOR

Shannon Steffee

ART DIRECTION

Yacinski Design, LLC

PRODUCTION MANAGER

Gretchen Gorfine

CONTRIBUTING EDITORS

Mark Brinkley, CIA, CFSa, CRMA
John Hall, CPA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Steve Mar, CFSa, CISA
James Roth, PhD, CIA, CCSA, CRMA
Paul J. Sobel, CIA, QIAL, CRMA
Laura Soileau, CIA, CRMA

EDITORIAL ADVISORY BOARD

Dennis Applegate, CIA, CPA, CMA, CFE
Lal Balkaran, CIA, CGA, FCIS, FCMA
Mark Brinkley, CIA, CFSa, CRMA
Adil Buhariwalla, CIA, CRMA, CFE, FCA
Daniel J. Clemens, CIA
David Coderre, CPM
Michael COX, FIA(ANZ), AT
Dominic Daher, JD, LL.M.
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, PHD
J. Michael Jacka, CIA, CPCU, CFE, CPA
Keith E. Johnson, CIA

Sandra Kasahara, CIA, CPA
Eila Koivu, CIA, CCSA, CISA, CFE
Robert Kuling, CIA, CRMA, CQA
Michael Levy, 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
Kenneth Mory, CIA, CPA, CISA, CRMA
Jack Murray, Jr., CBA, CRP
Hans Nieuwlands, CIA, RA, CCSA, CGAP
Cathlynn Nigh, CRMA, CSSGB
Michael Plumly, CIA, CPA
Jeffrey Ridley, CIA, FCIS, FIIA
Marshall Romney, PhD, CPA, CFE
James Roth, PhD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debra Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PhD, CPA
Glenn Summers, PhD, CIA, CPA, CRMA
Sonia Thomas, CRMA

Stephen Tiley, CIA
Tom Tocashi, CIA, CCSA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoor, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CFSa, CRMA

IIA PRESIDENT AND CEO

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

IIA CHAIRMAN OF THE BOARD

Larry Harrington, CIA, QIAL, CRMA, CPA



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.

IIA Audit Group Membership

Join. Save. Succeed.



Strengthen your entire team with an IIA Audit Group membership.
Organizations with as few as two auditors can save.

“My team is more efficient because of our group membership. With convenient and centralized resources for professional guidance, training, and networking, we are better prepared to take on any internal audit project with confidence.”

Timothy J. Sangiovanni
Manager, Internal Audit
Topperware Brands Corporation
IIA Audit Group Member Since 2013

To learn more about an IIA
Audit Group membership, go to
www.theiia.org/goto/group.



and the analytics function will shift to providing complex analysis and verifying the integrity of the analysis performed by the audit teams.”

DAVID CODERRE, author of “Gauge Your Analytics.”

Leave Our Comfort Zone

Richard Chambers’ blog post makes a lot of sense, and there are many CAEs who are “stepping up to the mark.” However, as he says, if we don’t take risks to add value to important risk matters as a profession, what risks might organizations take that they could later regret? A serious challenge for the profession is what to do when stakeholders are ignorant of the broader audit role and deliberately want to keep audit “in a box,” or when CAEs want to keep their “heads down”? It’s not self-evident to me that

nonexecutives always see the problem, and even if they do, whether they want the more progressive audit function Chambers is promoting (which I completely agree with). However, at some point I suspect the profession will need to address these challenges more systematically; otherwise, I can see us saying the same things in five years’ time.

J. PATERSON comments on the Chambers on the Profession blog post, “To Audit Emerging Risks, We May Have to Leave Our Comfort Zone.”

A Disconnect

IT is, at times, insular; IT security is even more so. That’s pretty widely recognized. As far back as 2001, we (CSO magazine) were writing extensively about not using FUD (fear, uncertainty, doubt) and speaking the language of the business. Yet, even at that, I wasn’t

really aware of “risk managers” as a corporate function until 2008, didn’t pay any attention to The Committee of Sponsoring Organizations of the Treadway Commission until maybe 2012, and so on. So, I wholeheartedly agree with Marks’ closing points, but there is a ton of silo-busting and educational work to be done. And the message will probably have to be carried by somebody very influential within the IT security “technical” community—someone who is already inside that echo chamber.

DEREK SLATER comments on the Marks on Governance blog post, “The Disconnect Between Information Security Officers and Executives.”



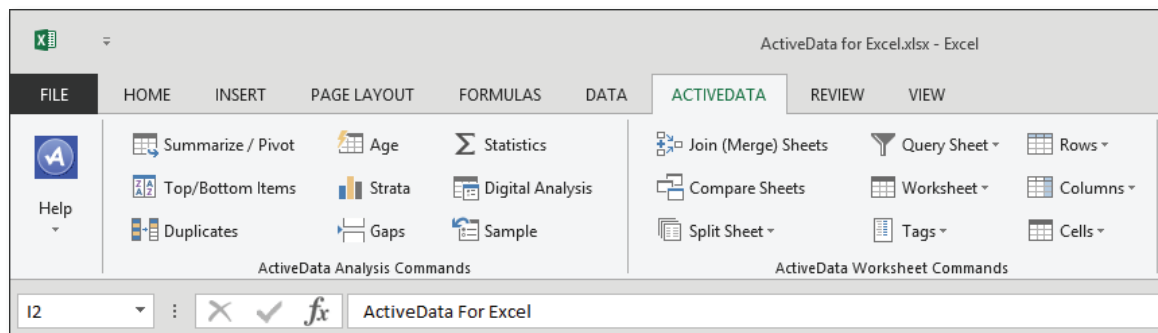
VISIT InternalAuditor.org for the latest blogs



ActiveData for Excel®

Computer Assisted Audit Techniques for Microsoft Excel

ActiveData turns Microsoft Excel into a powerful data analytics platform for auditors.



ActiveData delivers a comprehensive set of features at a fraction of the cost of existing CAATs solutions.

Download a free, fully functional 30 day trial from our website:

informationactive.com/iia

See us at the 2015 IIA GAM Conference, March 9-11 in Las Vegas

Microsoft Excel is a registered trademark of Microsoft Corporation



Join the Celebration!

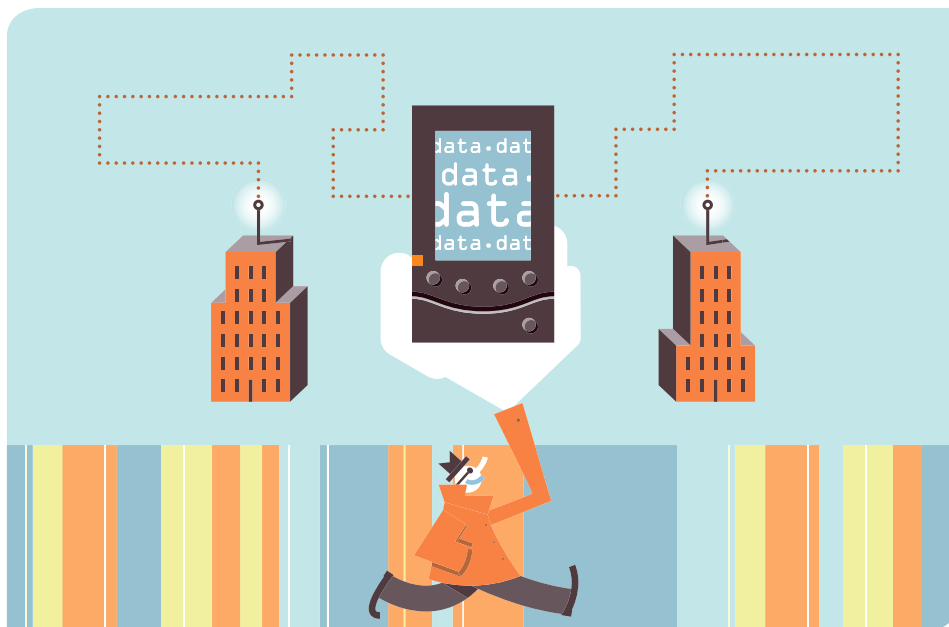
As we commemorate our fifth year of empowering CAEs in their unique and challenging roles, the Audit Executive Center® has grown to support more than 800 CAEs and more than 6,000 of their staff. The Center is THE go-to resource dedicated to what CAEs need to make them more effective in serving their customers, their stakeholders, and their own professional development.

Join Us!
www.theiia.org/cae



U.S. agencies' e-discovery struggle... Data governance responsibilities... Internal audit in state government... Nations failing to fight bribery.

Update



ACCOUNT FRAUD NEARLY DOUBLES

Fraudulent applications for U.K. current bank accounts rose sharply over the first two quarters of 2015.

Q1 **81** in every 10,000 applications were fraudulent.

Q2 **151** in every 10,000 were fraudulent.



Q1 **49%** of cases involved identity theft.

Q2 **69%** involved identity theft.

Source: Experian PLC

FRAUD KNOWS NO BOUNDS

Better sharing of data across industries and a universal language may help anti-fraud efforts.

Eighty-four percent of fraud mitigation professionals interviewed encounter fraud that crosses multiple industries in their investigations, according to the 2015 LexisNexis Fraud Mitigation Study. Of the 400 fraud mitigation professionals from insurance, financial services, retail, health care, government, and communications surveyed, 77 percent say fraud mitigation cases connected to another industry have a high or moderate financial impact on their organization.

“The fact that data is not yet better shared across industries reveals an exposure for organizations that are combatting

millions in fraudulent activities each year by individuals and organized crime rings,” says Bill Madison, CEO, insurance, LexisNexis Risk Solutions in Atlanta. “Status quo fraud mitigation is not enough for fraud schemes that are becoming increasingly sophisticated. Sharing more data will enable organizations to be armed with more effective tools in the fraud battle.”

More than three-fourths (76 percent) of those surveyed would use data from other industries as an indicator of potential fraudulent activities in a case they are investigating. Eighty-seven percent would find a universal and consistent way of describing

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



**70%
OF BOARD
MEMBERS**

say they understand the security risks to their organization.

**43%
OF IT
SECURITY
PROFESSIONALS**

say their board is informed about the organization's IT threats.

"The data shows that board members are very aware of cybersecurity, but there is still a lot of uncertainty and confusion – many lack knowledge not only about security issues and risks, but even about what has transpired within their own companies," says Larry Ponemon, chairman of the Ponemon Institute.

Source: Fidelis Cybersecurity and Ponemon Institute, Defining the Gap: The Cybersecurity Governance Survey

fraud across industries valuable. Moreover, 60 percent indicate it would be very valuable to have access to on-demand data about fraud activities, events, persons, or other attributes within their industry, and 41 percent say the same for information outside of their industry.

The survey also explored the use of data analytics in fraud detection, with 45 percent relying on external data and analytics-based

solutions very frequently and 75 percent relying on them to some extent. The biggest drivers of data analytics use are compliance (65 percent) and accuracy (54 percent).

"Having data analytics programs at the organizational level is very beneficial," Madison adds. He says fraud mitigation professionals can better attack the fraud problem if they are armed with insights and data shared across industries. **-S. STEFFEE**

E-DISCOVERY IN DOUBT

Poor technical and management support hinders e-discovery in U.S. government legal cases.

U.S. federal government professionals aren't confident in their agency's ability to manage e-discovery in legal cases, according to Deloitte's 2015 Benchmarking Study of Electronic Discovery Practices for Government Agencies. Three-fourths of respondents report their agency wouldn't be able to demonstrate that its electronically stored information (ESI) is "accurate, accessible, complete, and trustworthy."

Only 42 percent of the 149 U.S. government professionals surveyed—most of them attorneys—say they are prepared to discuss e-discovery matters with opposing

counsel, down from 56 percent in Deloitte's 2014 study. Moreover, 51 percent say they lack adequate technical support to prepare for such discussions.

"While the tools and technologies continue to mature along with our understanding of ESI, the expanding scope of the issue is daunting," Chris May, a principal with Deloitte Transactions and Business Analytics told *CIO Journal*.

Respondents say the top challenges government agencies face to identify ESI are insufficient manpower, insufficient time, and the volume of data the agency has collected. Challenges for handling, processing, reviewing, or producing ESI include internal systems and processes, budgetary issues and constraints, and top management buy-in. **- T. MCCOLLUM**

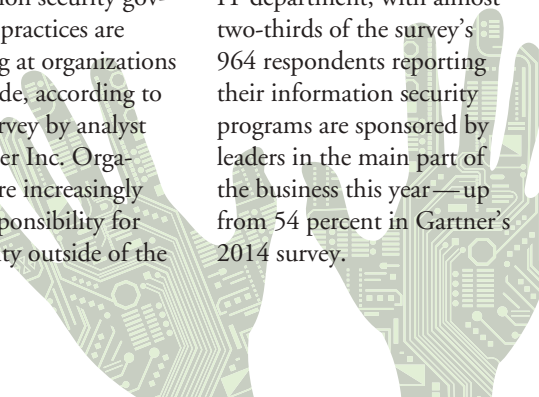
DATA SECURITY GOVERNANCE EVOLVES

More businesses view cybersecurity as a business risk.

Information security governance practices are maturing at organizations worldwide, according to a recent survey by analyst firm Gartner Inc. Organizations are increasingly placing responsibility for cybersecurity outside of the

IT department, with almost two-thirds of the survey's 964 respondents reporting their information security programs are sponsored by leaders in the main part of the business this year—up from 54 percent in Gartner's 2014 survey.

The research, Survey Analysis: Information Security Governance, 2015–2016, notes regional differences in organizational sponsorship. Fifty-seven percent of survey participants in North America indicate sponsorship from outside IT,



IMAGES: TOP, XIWINXING / SHUTTERSTOCK.COM; LEFT, DEBRA HUGHES / SHUTTERSTOCK.COM



Visit InternalAuditor.org to read an extended interview with Jacob Flournoy.

compared to 63 percent in Western Europe and 67 percent in Asia/Pacific. Respondents worked for companies with at least US\$50 million in total annual revenues for fiscal year 2014, with a minimum of 100 employees.

More than one-third of participants also indicate that the most senior person responsible for information security in their organization reports outside of the IT department. “The primary reasons for establishing this reporting line outside of IT are to improve separation between execution and oversight, to increase the corporate profile of the information security function, and to break the mindset among employees and stakeholders that ‘security is an IT problem,’” says Tom Scholtz, vice president and Gartner fellow. “Organizations increasingly recognize that security must be managed as a business risk issue, and not just as an operational IT issue.”

When asked about the effectiveness of their organization’s security policies, half the survey respondents say that a security governance body is involved in assessing the policies, though only 30 percent say the business units are actively involved in developing the policies that will affect their businesses. Although this is an improvement over last year’s 16 percent, Gartner notes it still indicates a lack of active engagement with the business. **-D. SALIERNO**

UP TO THE CHALLENGE

Jacob Flournoy, internal audit director at the University of Arkansas System, was recently honored by the American Institute of Certified Professional Accountants for building an internal audit function that has made a major impact on state government.



What were the biggest challenges you faced in starting the internal audit function at your organization?

The first challenge was addressing a backlog of requests for internal audit services. The board and senior management initially had a long list of areas in need of independent reviews and audits. It took a while to work through the audit issues disclosed in these areas. Other challenges included getting the right audit policies in place, obtaining sufficient resources for developing an internal audit function that could meet the *International Standards for the Professional Practice of Internal Auditing*, and staffing up with Certified Internal Auditors.

What impact has internal audit had on the organization since it launched? We serve as direct staff support to the board’s Audit and Fiscal Responsibility Committee and strive to write concise reports that will be read, understood, and acted upon for the benefit of the stakeholders and citizens that our organization serves. We bring the concepts of transparency, accountability, accuracy, efficiency, effectiveness, independence, and integrity into the forefront for assisting the university’s leadership in resolving the diverse and complex issues that come through the audit process.

FOOT-DRAGGING ON BRIBERY

Only four nations are actively prosecuting foreign corruption.

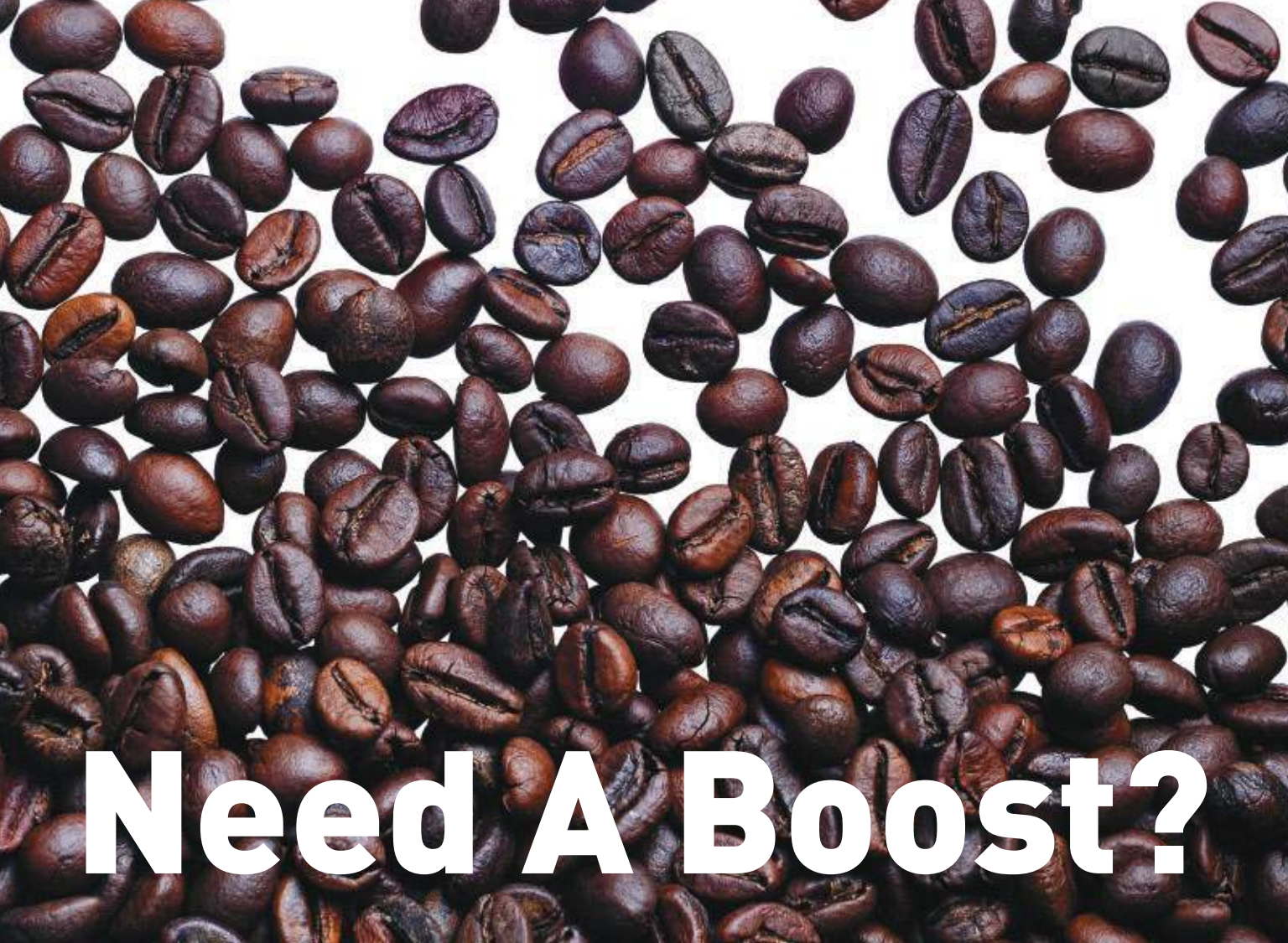
Most nations that have signed the Organisation for Economic Development and Co-operation’s (OECD’s) anti-bribery convention have not investigated or prosecuted a foreign bribery case in the past four years, Transparency International reports. These countries make up more than 20 percent of world exports, the anti-corruption advocacy organization asserts in its latest progress report.

Germany, Switzerland, the U.K., and the U.S. are the only anti-bribery convention signatory nations that have actively pursued anti-bribery cases during this time, the report notes. The four nations have completed 215 cases and started 59 new cases since 2011. The other 37 signatory



countries combined only completed 30 cases and started 63.

“The OECD must ensure real consequences for such poor performance,” says Transparency International chairman José Ugaz. “Violation of international law obligations to counter cross-border corruption cannot be tolerated.” Two barriers hindering legal efforts against bribery are insufficient sanctions in laws and political influence that impedes investigations. **-T. MCCOLLUM**



Need A Boost?

Harvest the Power of Spreadsheets

Embrace spreadsheets
Know your spreadsheets are risk free
Collaborate with a spreadsheet audit trail

Unmatched Visibility • Exceptional Control • Ease of Use

Learn more about spreadsheet risk management at incisive.com

Back to Basics

BY DAVID HARVEY + BERNICE LEMAIRE

EDITED BY LAURA SOILEAU + JAMES ROTH

CORRECTIVE ACTION PLANS

By advocating for timely correction of audit deficiencies, internal auditors can reinforce a strong control environment.

Internal audits identify internal control issues and opportunities for efficiencies, and make recommendations to reduce the potential for fraud, even in organizations with strong controls. Management must determine what action, if any, it will take based on the nature of the audit results, potential risks, and the cost and benefits of implementing corrective actions. A corrective action plan comprises step-by-step instructions that are developed to achieve desired outcomes cost effectively, such as addressing a deficiency identified during an internal audit.

Internal auditors should stress to management the importance of developing corrective action plans to address noted weaknesses, especially those with significant impact or materiality. The *International Standards for the Professional Practice of Internal Auditing* requires internal auditors to follow up on audit issues and evaluate

corrective actions, as stated in Standard 2500—Monitoring Progress and Standard 2500.A1, which says the CAE “must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.”

Internal audit departments may use a system to track audit issues as open or closed. Discussions with management are encouraged to help ensure that risks are fully understood and that potential corrective actions are appropriately considered. Once internal audit concludes that management has provided adequate evidence that a corrective action plan has been fully implemented, or follow-up testing shows necessary improvements, the audit issue can be closed. An understanding of the corrective action plan process promotes an effective audit cycle.

Planning and Development

Many internal auditors use a condition, criteria, cause, effect, and recommendation format in presenting audit findings. Understanding this approach can guide development of a quality corrective action plan.

Condition What was found during the audit? For example, “A contract employee included expenditures for alcohol on a travel voucher, and it was reimbursed as an expense despite the company policy prohibiting such reimbursement.”

Criteria What policy, rule, or regulation was violated, such as a company policy on expense reimbursement?

Cause What is the reason that the violation occurred? Was it lack of employee training regarding expense reimbursement? Lack of management review of invoices? Depending on the

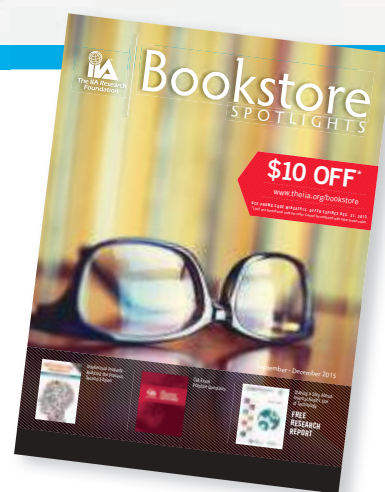
SEND BACK TO BASICS ARTICLE IDEAS to Laura Soileau at Isoileau@pncpa.com

Shop the Latest IIARF Bookstore Spotlights



Browse our selection of books from the Most Comprehensive Collection of Practitioner-reviewed content available anywhere and everywhere you go.

Update your internal audit library and save money: 10% off IIARF eBooks or \$10 off your total purchase. Offers expire Dec. 31, 2015.



Download and Shop IIARF's Bookstore Spotlights Now:
<http://www.theiaa.org/goto/bookstorecatalog>



TO COMMENT on this article,
EMAIL the authors at david.harvey@theiaa.org

nature of the issue, the root cause can be difficult to discern cost effectively.

Effect What is the impact? For example, how much did the company pay for the inappropriate expense?

Recommendation What would fix the problem? This should address the cause of the noted condition or the underlying risk with the goal of avoiding reoccurrence of the condition.

Ideally, the audit report should address the root cause or potential causes and underlying risks. However, management may need to obtain additional information in developing corrective action plans. Management should be able to answer:

- » What happened?
- » What should have happened?
- » Where was the process failure and what caused it?
- » Were there any contributing factors?
- » Who is accountable for the area in which the process failure occurred?
- » What was the operating environment in which the failure occurred?
- » What are the risks involved, what is the level of urgency, and what resources are available to address this issue?

Once these questions are answered, management can begin to develop the corrective action plan to address audit issues cost effectively and consistent with its risk appetite. Key practices in the corrective action process include:

- ➔ Identifying an executive or senior manager to oversee the corrective action plan process and to approve and monitor the corrective action plan. The nature and scope of the audit issue will be a key factor in the selection of the person to serve in this capacity, such as a chief operating officer or human resources director.
- ➔ Identifying potential solutions and determining the best choices based on available resources, time, and severity of the issue. It is helpful to document why alternative solutions were not adopted, such as they were too costly or not feasible because of technological limitations.
- ➔ Assigning a manager to develop the corrective action plan and to present the plan for approval to the executive or senior manager with oversight responsibility.

The level of detail and complexity of the corrective action plan can vary widely, though there are important considerations when developing the plan: specific steps that address the root cause; milestones with achievable deadlines and identified lead persons; legal/regulatory requirements; steps for training, policy and procedure updates, testing, etc.;


resource needs (e.g., new hires, cost to develop or update procedure manuals, and IT system redesign); and major assumptions and dependencies.

Implementation and Monitoring

Progress toward corrective action plans should be regularly monitored, and explanations for delays or cost overruns should be sought. The plans should be modified when warranted because of changes in systems, resource availability, or other factors. Several practices should be considered:

- ➔ Management should maintain a database of all audit issues, or request reports from such a database maintained by internal audit. Status reports regarding corrective action plan steps should be regularly provided to stakeholders, and additional focus should be placed on high-risk areas and those actions that are overdue.
- ➔ Once corrective actions have been implemented, management should ensure that any necessary updates to policies and procedures are completed, and that employees are made aware of new procedures or receive training on them.
- ➔ Internal audit should coordinate with management about communications regarding remediated audit recommendations. One option would be to request that management develop a package of materials documenting the corrective actions taken. Such a package could be reviewed by internal audit, or be made available during follow-up reviews. In addition, the package could serve as a resource for external auditors performing the annual audit of the financial statements.

A Strong Control Environment

Timely follow-up of audit deficiencies is important to internal auditors as well as management. Such audit deficiencies should be taken seriously, or the organization may suffer consequences. Developing and effective implementation of corrective action plans, and being able to document actions taken, promotes a strong control environment. Proactive consideration of the underlying risks and ongoing monitoring by management to ensure that corrective actions remain effective are critical to the corrective action plan process. Follow-up audits by internal audit help ensure accountability and provide management an independent feedback loop. 

DAVID HARVEY, CIA, CPA, CMA, CGFM, is deputy director, contracts and controls review, at Pension Benefit Guaranty Corp. (PBGC) in Washington, D.C.

BERNICE LEMAIRE, CIA, CPA, CGMA, CFE, is the chief auditor, benefits administration and payment, at PBGC.

SHUTTING THE DOOR ON SOCIAL ENGINEERING

Internal audit can help organizations thwart efforts to manipulate employees to gain system access.

A busy senior executive walks into her office on Monday morning and begins to review her email. About halfway through, she sees this message:

To: All employees
From: HR and IT department

The IT department has contracted with XYZ Consulting to test and enhance the performance of our network. In doing so, we ask that you sign into the link below and run a few tests. XYZ has asked us to get as many people as possible to perform the tests to get a true reading of our network speed. Your help is greatly appreciated. Link here: <http://xyznetworktesting.com>

The executive finds it odd that she was not informed about this project and calls the IT department to find out more. She is stunned to learn that not only did IT not sanction any network testing, but that this

is a phishing email and more than 100 employees had clicked the link and signed in with their network credentials before IT could stop it.

This scenario is a good example of social engineering in today's highly connected business environment. Wikipedia describes it well: "Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information."

CAEs have an interest in knowing how the information security department addresses social engineering, primarily because it is used to perpetrate fraud. Additionally, internal audit should proactively assist in detecting how these techniques play out in their organization and help deter them.

How It Works

Social engineering usually targets communications systems. The most common method is to send a phishing

email that asks the user to click on a link. This link is set up by the perpetrator to request a user's network ID and password, thus obtaining the needed credentials to access the company's systems and data. The scammer then uses those credentials to sign onto the system legitimately, access confidential information, and download the information to sell or perpetrate fraud.

Some social engineering approaches are elaborate. One variation is to have the link execute a piece of malware to invade the system. Another variation is to offer an incentive to entice the user to click on the link such as money or scheduling a package delivery. Still another technique is for the sender to say he or she is acting under the direction of the IT department or a senior executive. Some scams play on a user's personal situation or sympathetic side—a compassionate plea about a sick

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



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

child or parent—to trick the user to click on a link or go to a fraudulent website. Some of the nastiest scams—particularly in the banking industry—send phishing emails purporting to be from the organization that tell its customers they need to refresh or verify their credentials or their accounts will be closed.

Although the email system is the main target, scammers can use the telephone system, as well. For example, a scammer can call claiming to be a customer who has lost his or her credentials to access his or her account. Or callers might say they need to access their financial account immediately and don't have time to verify their personally identifiable information. Another technique is to call an employee claiming to be

Do not allow executive privilege to dictate email policy.

a consultant working on the system who needs the employee's credentials to fix something on the system.

What Internal Audit Can Do

Addressing social engineering is not a task internal audit can tackle on its own. But there are things auditors can do to help the information security department protect the organization.

Testing Performing a social engineering audit in conjunction with the information security department is one of the most effective and eye-opening things internal audit can do to discover whether the organization has a large-scale awareness issue. A good social engineering test consists of:

- Craft a phishing email similar to those used in common phishing scenarios.
- Work with IT to set up a fake Web address where the link should be directed.
- At the website, ask for sign-in credentials.
- Send the email to employees and monitor who clicks on the link and enters their credentials.

Awareness Work with the human resources (HR) and information security departments to develop an effective information security awareness program. Employee awareness is the No. 1 way to deter email and phone phishing scams. Teach employees that while customer service is important, they should never bypass information security protocols to help customers unless they have verified through established procedures that they are truly communicating with a customer.


Hotline Include suspicious emails in the organization's fraud reporting hotlines and procedures. Detecting fake emails is just as important as uncovering an employee who is misappropriating funds. The only difference is they are using a different means to perpetrate the fraudulent activity. One way to encourage reporting is to place an icon on the email tool bar that allows users to easily report a suspicious message.

Audit Procedures Include questions in audits that ask about any unusual activity related to emails or phone calls. Giving system credentials to strangers is even worse than sharing credentials with other employees.

In addition to these items, advise information security and HR to enact these procedures:

- Do not allow personal email to be sent to or from work addresses. This limits the number of suspicious emails and helps deter internal fraud by disgruntled employees emailing sensitive company data to their personal email.
- Monitor all email sent to noncorporate email addresses.
- Recommend tools that have aggressive and effective spam filters to weed out spam and emails sent out through automated email generators.
- Enforce a formal email or computer use policy.
- Do not allow executive privilege to dictate email policy, which can circumvent the measures the information security function has implemented to protect the organization. Executives and senior managers are just as likely as other employees to click on a phishing message.
- Never pre-announce social engineering tests. The element of surprise is important. Testing the awareness level will only be successful if it's performed under true conditions.

Minimizing the Threat

Internal audit has a role to play in an organization's social engineering defenses. While it is primarily an information security responsibility, awareness, monitoring, and setting up and recommending controls are all activities that internal audit can actively be involved with to minimize the chance that the organization's systems are breached. In addition, auditors should help detect and minimize conditions that exist for social engineering fraud. Cybercrimes are now one of the new "misappropriation of assets" frauds within organizations. The asset being misappropriated is customer and company private information, and the repercussions to the organization can be devastating. 

KEN PYZIK, CISA, is an independent IT audit, compliance, and project consultant in Las Vegas.

Our promise.



Our guarantee.

Revenew provides the only comprehensive “procure-to-pay” audit solution in the marketplace today. Our Contract Compliance Audits – self-funded and backed by a Performance Guarantee – yield tangible results with impactful process improvements. We are proud to say that every one of our clients is available to tell you that we deliver what we promise. Review case studies and see what our clients have to say at www.revenew.net/promise.

Fraud Findings

JOHN L. VERNA + CHRISTOPHER T. MARQUET EDITED BY JOHN HALL

THE ABUSE OF EXECUTIVE POWER

An inattentive board of directors allows a CEO's wrongdoings to go unnoticed.

It was 9:35 on a Wednesday morning in New York at the board meeting of a multi-billion-dollar, publicly traded company. The CEO, Richard Tompkins, was in a rage. The chairman of the board had just told him to resign or he would be fired. Tompkins' reaction was classic, immediate, and violent. He was the shareholders' greatest nightmare.

Tompkins was brought in to execute the turnaround of the company and initially had done a reasonable job. He claimed he needed a team he could trust and did not have time to evaluate the existing group, so he brought in a new chief operating officer, chief financial officer (CFO)/controller, chief information officer, human resources (HR) director, general counsel, purchasing agent, CAE, and external auditor—all friends and former colleagues. The board, anxious for the company to be saved, voted in favor of every organizational

change Tompkins steam-rolled through. But over the next several years, rumors of executive abuse began, including insider land deals and related-party transactions, excessive equipment and service purchases from related parties, unusual consulting contracts, inappropriate personal expenses, personal use of the company airplane, extravagant golf outings and parties, unnecessary foreign travel, and company vehicle abuse.


During this period, even the chairman, who was busy with other ventures, took little time to fully understand what was going on inside the company. Meanwhile, the internal auditors, while formally reporting to the audit committee, were under the day-to-day control of the CFO, Tompkins' close friend. As long as the earnings looked good, the board was happy to show up and vote "present."

When the recession took hold and revenues dried

up, multiple frauds began to surface, rounds of layoffs commenced, and whistleblower calls started pouring in to the HR director, with no effective or independent follow-up. The calls then were diverted to corporate counsel, who wrote them off as disgruntled former employees, assuring the chairman that there was no basis to these unfounded allegations. The audit committee chairman, an outside member of the board brought in by Tompkins, put his faith in the audit system and did not give the disgruntled former employees adequate consideration.

All these activities finally came to light because of Harriet Stevens, a quiet and humble accounts payable employee who identified a US\$2.5 million bridge construction project over the company's pond that was awarded to the CEO's son, a building contractor. Stevens first called the company's ethics hotline. When

SEND FRAUD FINDINGS ARTICLE IDEAS to John Hall at john@johnhallspeaker.com



Unmanaged risk can topple the delicate balance of your organization

Navigate business risks & opportunities with **Risk-Intelligent Audits**

MetricStream's audit management solution helps organizations:

- Align audit to the right set of business risks
- Improve relevance, credibility and transparency of audits
- Ensure optimal resource utilization and effectiveness
- Simplify compliance with embedded regulatory content & standards
- Drive efficiency & collaboration with an integrated audit system





TO COMMENT on this article,
EMAIL the authors at john.verna@theiia.org

nothing happened after her report, she called the chairman of the board.

The chairman was independent of management and the largest shareholder in the company. His interests were well aligned with the shareholders. He called in independent investigators, which he initially paid for out of his own pocket. As the inside business process consultants reviewed company operations, they fed the outside team with various leads, which allowed the investigators to identify and target various companies and individuals for investigation and approach. This effort, combined with the numbers coming from the inside team, allowed the investigators to identify and document numerous serious irregularities and outright frauds perpetrated by Tompkins and his cohorts.

Tompkins' multiple frauds were successful—at least for a time—because he had complete and unquestioned control over the day-to-day operations of the business, including the ability to circumvent existing weak controls. Tompkins was able to pack the company with yes-men and friends—some of whom actively participated, enabled, or otherwise conspired with him in several frauds. The external auditors were completely ineffective in probing deeply enough to ferret out the misdeeds. They were eager to maintain their new Fortune 100 client and did not want to rock the boat. Consequently, they failed to recommend a stronger and tighter business control structure to prevent some of the shenanigans. While the outside auditors were aware of the internal control weaknesses surrounding Tompkins' inappropriate activities, they failed repeatedly to directly confront these issues.

The board was little more than a rubber stamp for Tompkins. Whatever he did in the name of saving and running the company was always approved. All of the independent directors sat on multiple boards, leaving them insufficient time to direct and monitor the company's executives. Several lacked the depth of skill to understand the company's operations and competitive position. In particular, the audit committee chairman placed far too much reliance on the work and opinions of the outside auditors and the CFO.

During the early phases of the CEO's irregular activities, the magnitude of the transactions fell far below the "materiality levels" of the outside auditors. This fact, combined with the CFO's willingness to hide questionable spending within the forest of the company's transactions, effectively camouflaged the CEO's activities.

The board was faced with a vexing dilemma. It needed to decide whether to pursue criminal or civil action against the CEO or let him go quietly to avoid a scandal, which would negatively affect the shareholders. In the end, it chose the quiet path.

Lessons Learned

- The chairman is, or should be, the chief advocate for the shareholders, and completely independent of management. It is the chairman's primary job to direct the company's executives and drive oversight of their activities in the name of the shareholders.
- An independent and highly skilled audit committee chairman is essential to maintain a robust system of checks and balances over all operations. To be truly effective, the chairman must be independent of those he or she is charged with watching.
- The CAE must report to the audit committee and have his or her budget, compensation, mission, career path, and hiring/firing authority fully insulated from executive management.
- The chairmen of the board and the audit committee must devote material time to their duties. While the board can use the company's oversight functions to maintain a checks and balances process, there is no substitute for personal, direct involvement.
- The board must be willing to direct inquiries into allegations of misconduct, and have unquestioned confidential spending authority to conduct reviews and investigations as it deems necessary.
- One of the most effective compliance tools available to the board is the day-to-day vigilance of the company's employees. When an individual employee detects wrongdoing, he or she must have an effective and safe method to report observations, such as a third-party ethics hotline that reports to the chairman of the board and audit committee. All employees must be protected from retribution to avoid any possibility of corrupting the process.
- A zero-based budgeting process—requiring that the individual elements of the company's budget be built from the bottom up, reviewed in detail, and justified—would have facilitated the identification of unusual spending in numerous corporate and operating units. This provides an in-depth view of spending as opposed to basing the current year's spending, in aggregate, on last year's spending, where irregularities may be buried and overlooked.

JOHN L. VERNA, CBA, CPA, CFE, is founder and executive director of the Center for Strategic Business Integrity in Washington, D.C.

CHRISTOPHER T. MARQUET, CBA, is managing director and head of research for the Center for Strategic Business Integrity and the CEO and founder of Marquet International Ltd. in Wellesley, Mass.

Defense

Charles Perrow may not be a household name today, but his book, *Normal Accidents*, raised hackles in organizational sciences circles in the mid-1980s by suggesting that accidents happen in complex organizations. In Perrow's view, people know they are not perfect and neither are machines, so they compensate by adding layers of redundancy—making those systems complex. Generally, the

layers are not independent of each other, which limits their effectiveness. Moreover, when people know redundancy exists, they tend to relax their vigilance and assume someone else is on full alert. However, Perrow suggested a solution: The weaknesses can be mitigated by defining clear and consistent roles and responsibilities, and maintaining separation among these roles.

These concepts may seem obvious to anyone in internal audit, given the profession's longtime propensity for clarity and independence. In 2013, The IIA formalized these practices in

Jane Seago

in depth

the position paper, *The Three Lines of Defense in Effective Risk Management and Control*.

The IIA recognized a need for a simple, streamlined, effective way to organize the many facets of risk management and internal control in 21st century organizations. Businesses had become more complex and connected, and the number and types of potential risks had increased commensurately. More risks necessitated more roles in

the company to monitor and mitigate them. Organizational charts had taken on a decidedly spaghetti-like appearance, with overlapping and crisscrossing lines of reporting and communication. A lot of activity was going on, but a methodology was needed to ensure it was accomplishing the desired results.

“In financial services, risk management is a competitive advantage,” notes Robert Croft, executive director, internal audit, for Nomura, a global financial services group based in Asia. “We need a model that enables the whole organization to understand the

Organizations that have adopted the three lines model experience collaborative opportunities to address risk.

risks and who is managing the risks, and respond to the rapidly changing business and regulatory demands. Our operational approach to managing and overseeing risks is conducted with a common framework and language—the clearly articulated IIA model, which provides a rigorous and efficient approach to discussing risk and control.”

THE THREE LINES

The IIA’s three lines of defense model describes three layers to identify and manage risk, based on position, role,

and responsibilities within an organization. The first line, operational management, is based on the management and internal control measures designed into systems and processes. This line comprises the business and process owners whose activities identify, assess, control, and mitigate the risks that can facilitate or prevent achievement of the organization's objectives. They not only own and manage risk, they also are responsible for implementing corrective actions to address process and control deficiencies.

The second line monitors risk and compliance and is a management and oversight function. It applies additional expertise, process knowledge, and monitoring to support the actions of the first line of defense, while remaining separate from it.

Internal audit is the third line, with primary responsibility for providing assurance directly to senior management and the board of directors about the other two lines' governance, risk, and control efforts. Complete objectivity and independence are integral to this role, so the third line operates as an assurance, not management, function.

Doug Anderson, executive-in-residence at Saginaw Valley State University in University Center, Mich., and CAE subject matter consultant for The IIA's Audit Executive Center, says the primary benefit of using the model is in its very nature. "Fundamentally, it's a governance model," he explains. "It tells organizations how they should structure themselves so they can manage risk. That sort of governance helps an enterprise achieve its objectives."

The IIA's model does not include the board of directors and equivalent governing bodies or senior management among the lines of defense. Instead, they are considered stakeholders served by the three lines. However, because they are responsible for setting organizational objectives and establishing structures to manage any risks arising from

the pursuit of those objectives, they play an important role in risk and control.

Two other groups sit outside the model, while still having a major effect on its operation: regulators and external audit. These groups can be considered another type of defense, but their scope is generally too narrow to align with the overarching nature of the three lines.

A SHARED OBJECTIVE

Although it is natural to focus on how the three lines differ, they have key similarities, as well. Their stakeholders are the same, as are their risk and control issues. They share the ultimate aim of helping the organization achieve its objectives while effectively managing risk. Their differences enable them to work efficiently; their similarities ensure they are working effectively.

Susan Holleran, vice president of audit and risk management at Waters, an analytical laboratory instrument manufacturer in Milford, Mass., appreciates the importance of the similarities in a governance, risk, and controls (GRC) project. "Several years ago, we began looking at GRC within the organization on a global basis to determine all the places we had some type of assurance-based functions," she explains. Her group looked at areas such as finance, IT, environmental health and safety, human resources, quality, and regulatory affairs. "We asked ourselves what these people were measuring and monitoring, and who their constituents were," she says. "Everyone was reporting and measuring within their own silos, missing the fact that much of what they were doing affected, or could be highly useful to, other parts of the organization."

Although this was before the three lines model was codified in The IIA's position paper, internal audit used exactly those same concepts to educate the Waters employees. "We made sure people understood where



“[The model] tells organizations how they should structure themselves so they can manage risk.”

Doug Anderson

75% of CBOK respondents familiar with the **three lines** model say their organization has adopted it, but among those participants, 18% say distinctions among the lines aren't clear.

PUTTING A COSO FILTER ON THE THREE LINES

Doug Anderson of Saginaw Valley State University recently took a look at the three lines of defense model from the point of view of The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) updated *Internal Control-Integrated Framework* and notes how well the model and framework align. "The COSO framework talks about what needs to be done through the five elements of internal control," he says. "The three lines model talks about who should be doing it. It is critical to get those roles and activities right, and referring to both sets of guidance can be helpful in doing that."

Susan Holleran says Waters has implemented COSO 2013, and she recommends organizations take a close look at its guidance. She explains that it "gives us a more expansive view of our reporting—financial and nonfinancial, internal and external. It has also provided a more focused approach on the overall entity-level controls and understanding the cross-functional relationships within the organization."

*For more information about how the model and COSO 2013 align, download The IIA's white paper, *Leveraging COSO Across the Three Lines of Defense*, at www.theiia.org.*

the similarities were," she says. "We are a lean organization, so we needed to leverage our limited resources to drive efficiencies, but also it was important for management to understand the risk environment of the organization as a whole. If you manage within silos, how can you have a grasp of the full range of risks enterprisewide and understand the interdependencies and impact on the organization?"

AN ADAPTABLE APPROACH

While the model's structure is specifically defined, it is not inflexible. It lends itself to adaptation to support organizations of various sizes, structures, and complexity. Ultimately, regardless of how the model is implemented, the key is ensuring that all functions are operating in concert to achieve organizational objectives, avoiding gaps in coverage and duplication of effort. Of course, therein lies the challenge.

Steve Jameson, chief internal audit and risk officer with Community Trust Bancorp in Pikeville, Ky., knows that

challenge well. "Internal audit, loan review, compliance, and security report to me, and I also coordinate enterprise risk management," he explains. "There is an officers risk committee of risk champions that makes decisions about enterprise risk management (ERM). So, the third line of defense and some key second lines of defense—most of the groups that provide various types of assurance to management and the board—report to me."

Moreover, Community Trust has a board-level audit and asset quality committee (internal audit and loan review) and a risk and compliance committee (ERM, compliance, and security) to which Jameson reports and whose meetings his managers attend—facilitating maximum coordination. Overlaps are avoided because of "established charters, committee-approved work plans, and common reporting relationships," he says. "Independence is managed by established safeguards that are documented and reviewed annually with both the audit



We need a model that enables the whole organization to understand the risks and who is managing the risks."

Robert Croft



Independence is managed by established safeguards that are documented and reviewed annually."

Steve Jameson

committee and the board, and both bodies formally approve this framework and my role.”

Other organizations may not always be able to clearly define three separate lines of defense. “In a Utopian world, every organization would have clear delineation among all three lines,” says Thomas O’Reilly, director of internal audit at Analog Devices, a semiconductor manufacturer in Norwood, Mass. “But companies are always looking to reduce costs to achieve financial targets, and one way is head count. So, it’s important in smaller or leaner organizations for internal audit to play a prominent role and, to the extent possible, remain

independent of other activities in the enterprise, to be able to provide assurance that the first and second lines are performing effectively.”

This is not to say that achieving this outcome is always easy. O’Reilly says he understands how organizations might struggle with gaps or duplications among the three lines, but reiterates that “internal audit has a unique, enterprisewide view, and if it is truly a risk-focused department, it should have a good understanding of the operations and connections among all departments. This positions internal audit to identify gaps or duplication in risk coverage, especially in a decentralized company.”

CLARIFYING BLURRED LINES

Croft explains that employees at Nomura are introduced to the three lines model from their induction training and are familiar with their function’s role. Management promotes a culture of proactive risk management and reinforces individual responsibility for doing so. He elaborates, “Within the three lines framework, the lines of defense are defined, the individuals operate in their roles as risk managers, and, subject to independence and fulfilling their independent roles, the three lines work together to achieve Nomura’s objectives.” He acknowledges that tensions implied in the model sometimes do manifest themselves; however, when they

DEFENSE, OR OFFENSE?

Although the three lines model’s defense-in-depth approach has proven effective, some practitioners have argued that it should be about three lines of offense, rather than defense. Doug Anderson disagrees. “That opinion comes from those who think the model focuses on the downside of risk and fails to recognize its upside,” he says. “They point out, rightly, that an organization cannot achieve its objectives without taking risks. But the model is not only about reducing or eliminating risk—the model is not that restrictive. It’s about managing risk and properly sizing controls.”

Anderson notes that management generally doesn’t need a lot of prodding to take risks. If anything, managers can sometimes be too aggressive. “The model helps the organization achieve its objectives by taking—in a managed way—the right risks that are within the approved risk appetite,” he explains. So, while he understands the view of those who suggest a “three lines of offense” approach, he doesn’t agree with that terminology. “Maybe it’s three lines of *something*,” he reflects, “but I haven’t heard a better term.”

Thomas O’Reilly suggests “three lines of engagement.” He points out, “Risk management should address thinking clearly about risk and making good decisions to take risk, not run from it. I don’t talk to management about taking risk or avoiding it, but rather what the roles and responsibilities are, as related to risk. The model facilitates that discussion.”

EY’s Paul van Kessel says the debate is actually about something else. “I don’t think the people advocating the word ‘offense’ mean that they want organizations to harm others (offense); they want to protect their business (defense),” he explains. “The real question is whether the defense is reactive, proactive, or both. In the past we have focused on reactive. We learned from incidents in the past, and we put controls in place to avoid similar incidents in the future.”

In van Kessel’s view, today’s approach is more proactive in two ways: “We build risk management into our decision-making to make sure that we not only avoid the downside of risk but also benefit from its upside, and we collect intelligence in the market to make sure that we see incidents coming before they occur.”





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

do, “avenues exist to escalate discussions to help generate improved outcomes.”

Anderson notes the approach to the model can differ based on various organizational characteristics. “For example, because of the intense regulatory oversight focused on financial services, those enterprises generally have a more mature model,” he explains. “In smaller, less mature organizations, or those operating in a less regulated industry, we see more cloudiness about what tasks go where.”

Although the model allows for considerable flexibility, it requires effort to make it work within the organization and difficulties can be encountered. For Croft, positioning divisions that have both a producing/ownership role and an oversight role can be problematic. “Some firms are addressing the blurred margins between the lines of defense by adjusting the number of lines of defense,” he adds.

Jameson says turf battles can occur when the three lines don’t report to the same executive. “Some smaller organizations are still trying to catch up on establishing and fully resourcing all the lines of defense and creating the appropriate reporting relationships,” he notes.


Paul van Kessel, global managing partner of EY’s risk services in Amsterdam, says a possible explanation for such difficulties is that, although the model appears simple, few organizations understand they need a solid foundation before they can build the three lines of defense. “They need a strong risk culture across the organization; a clear definition and communication of risk appetite by the board or executive management; a standard language or methodology for identifying, evaluating, measuring, and reporting risk; a robust governance, risk, and compliance system; and several other factors in place,” he elaborates. “Meeting these requirements is hard work and is often seen as ‘something we will do in the near future.’ That is a big

mistake, and, in practice, the largest source of failure.”

TOWARD BETTER OUTCOMES

Given the effort involved, why should an organization implement the three lines model? Van Kessel points to a long list of issues that lead to incidents and motivate organizations to look to the model for a solution. Among them are complex and inconsistent reporting, gaps in risk coverage, siloed risk functions, business fatigue, confusion, and layers of redundant controls. “The resulting incidents can be significant, such as damage from risk you didn’t know you had,” he explains, “as well as confusion and embarrassment when talking about risk and risk management with the audit committee, shareholders, and regulators.”

While the three lines of defense model offers clear, tested guidance, organizations must find the best way to make it work for them. Organizations may not end up with a structure that exactly mirrors the model’s defined approach, but those that apply its principles can realize a more purposeful way of managing risk and internal control. “The way Community Trust has set up its three lines of defense is probably more of a blended model than a pure or traditional model,” Jameson notes. “But our board, management, external auditors, and regulators all like it.”

O’Reilly says rather than thinking of The IIA’s position paper as something management *has* to comply with, organizations should use it as a guide to help everyone in the business manage risk better. “When employees understand their risk and control responsibilities, we in internal audit can do our jobs better and the company benefits,” he says. “It’s hard to beat an outcome like that.” 

JANE SEAGO is a business and technical writer in Tulsa, Okla.



When employees understand their risk and control responsibilities, we in internal audit can do our jobs better.”

Thomas O’Reilly



The real question is whether the defense is reactive, proactive, or both. In the past we have focused on reactive.”

Paul van Kessel





Ask the Experts

Let **IIA Quality Services** be your resource for implementing a comprehensive Quality Assurance and Improvement Program to include **External Quality Assessments** that meet the requirements of The IIA's *International Standards for the Professional Practice of Internal Auditing* and provide insights for exceeding stakeholder expectations.

Get the Results

Contact us today for a free no-obligation proposal at quality@theiia.org or +1-407-937-1430.

In today's environment, an effective quality assurance and improvement program (QAIP) is critical to ensuring that internal audit meets the requirements of the audit committee, executive management, and other stakeholders. Internal and external assessments are key parts of the QAIP, and a robust QAIP incorporates many elements that are part of an organization's day-to-day activities. The IIA Practice Guide, Quality Assurance and Improvement Program, states, "Quality in internal audit begins with the structure and organization of the audit activity. Quality should be built into, and not onto, the way the activity conducts its business—through its internal audit methodology, policies and procedures, and human resource practices." By embedding quality into processes, rather than treating it as extra work, external quality assessments (EQAs) become a turnkey operation.

Fannie Mae has approximately 106 internal audit employees, performing 95 to 110 audits per year. A professional practice group comprising six full-time employees administers the QAIP. The group also is responsible for internal operations and reporting, and approximately 50 percent of its time is focused on the QAIP.

The QAIP is a regulatory requirement whose scope covers all operations of the internal audit department, including audits, reviews, audit issue follow-up, and special projects. Most of the program's components have been in place since before 2007; however, heightened requirements for financial services companies and the internal audit profession require Fannie Mae Internal Audit to continually refine and expand the program.

Because of the size and complexity of the enterprise, and to demonstrate continued compliance with The IIA's

The Value of QAIP

Fannie Mae's quality program demonstrates the effectiveness of its internal audit operations in meeting stakeholder expectations.

Margaret Ulvi

International Standards for the Professional Practice of Internal Auditing (Standards), internal audit has had an EQA performed more often than the required five-year period. In the 2014 EQA, internal audit received the highest rating—Generally Conforms—from The IIA’s Quality Services team. Before that, audit’s last EQA was in 2010, and going forward, it plans to have one performed every three years.

Fannie Mae considered several processes when looking at the overall quality of its internal audit function. And while process design may differ from organization to organization, having these processes in place is a key step toward building a high-quality department.

INDEPENDENCE AND OBJECTIVITY

To strengthen independence, Fannie Mae’s CAE reports directly to the chair of the audit committee and administratively to the CEO. Additionally, the audit committee sets the CAE’s compensation, and the audit department has goals that are completely separate from those of the overall organization.

An independence and objectivity policy provides required actions related to various situations that may lead to potential impairments, including the transfer of the CAE or audit staff from the business units into the internal audit department, cosourcing engagements, an auditor’s personal relationship with a member of the business unit being audited or consideration of employment with a business unit, scope limitations, and consulting/advisory engagements.

All internal transfers to internal audit complete an independence questionnaire to identify areas where there may be a conflict affecting objectivity. If a potential conflict is identified, the auditor is prohibited from participating in audits of that area for 12 months. This is monitored through a potential conflicts log that is reviewed in conjunction with scheduling. A

similar independence questionnaire is completed by any cosource or staff augmentation personnel that is considered before bringing the resource on board. As an additional protection, each assurance engagement includes an assessment of the objectivity of the engagement team members. This assessment is documented in the engagement workpapers.

Finally, audit personnel receive annual training on the policy, the *Standards* related to independence and objectivity, and The IIA’s Code of Ethics. Audit personnel also certify annually their compliance with the Code of Ethics. The results of the objectivity process form the basis for the CAE’s annual confirmation of the independence of the department to the audit committee.

STAFF DEVELOPMENT

Fannie Mae Internal Audit’s training program starts with an annual competency assessment to provide a structured guide enabling the identification, evaluation, and development of interpersonal, general, and technical capabilities of individual employees. Each category includes multiple competencies with specific measures identified for each competency. Interpersonal competencies include teamwork/collaboration, communication, driving execution (appropriate prioritization and achieving results), and inspiring/motivating. General competencies include critical thinking, business acumen, documentation, and project management. Technical competencies include mortgage business knowledge, enterprise risk management, and cybersecurity.

Each employee performs an annual self-assessment, and managers assess each person on their team. The manager and employee meet to discuss differences in their assessments and any gaps between where the employee was assessed and the expected rating. These gaps are considered while developing the employee’s annual training plan.

When all assessments have been completed, an analysis is performed by the professional practice group to identify competencies where 15 percent or more of employees have gaps in expected and actual assessed competencies. These competency gaps are an input to the annual department training schedule. Through internal development, or identification of an external training course, internal audit seeks to improve the department’s knowledge and skills related to any competency with a significant gap.

A training plan detailing the courses that will satisfy the employee’s 40-hour continuing education requirement and the breakdown of hours among competencies is developed by each employee (and reviewed by his or her manager) in conjunction with the performance management and goal-setting process. The professional practice group develops a training schedule or menu, considering results of the competency assessment, any significant changes in internal audit methodology, risks facing the enterprise, and results of the prior year’s quality assurance (QA) reviews. The plan is revised as needs change throughout the year. The competency assessment and training plan strengthens the performance management process and the QAIP. Additionally, employees appreciate the visibility into expected competencies and capability at each level provided by the competency assessment criteria.

RISK ASSESSMENT

Fannie Mae’s risk assessment process includes an annual risk assessment, a re-baseline of the annual risk assessment at midyear, and a continuous risk assessment (CRA), which is formally documented in the quarters during which the annual and re-baseline risk assessments are not performed. The annual and re-baseline risk assessments have various deliverables, including a

Surveys of audit clients are the most common tool used to support quality and performance processes, according to the CBOK 2015 Global Internal Audit practitioner survey.

revised audit plan; whereas the deliverable for the CRA is an updated watch list that includes key risk considerations identified and their impact on internal audit activities (e.g., covered in an existing audit or additional monitoring, or the addition of a new project to the audit plan). The presentation to the audit committee to support approval of the annual audit plan includes a list of key focus areas for the year; charts with project risk and type trends, plan hours by audit area, and plan hours by risk rating; and an audit plan resource analysis. The results of the CRA are not directly shared with the audit committee and management; however, any significant changes to the audit plan as a result of the CRA are.

METHODOLOGY DOCUMENTS

Methodology documents include methodology manuals, internal practice advisories and practice guides, standard audit programs, and required templates, which are incorporated by reference into the methodology manuals. Methodology manuals outline the basic requirements for internal audit's activities and cover the risk assessment, planning, fieldwork, and reporting phases of audit engagements, as well as audit issue follow-up and quality management. Fannie Mae practice advisories expand on internal audit's approach and related criteria for specific areas such as sampling, fraud risk assessment, and acceptance of risk, while Fannie Mae practice guides provide step-by-step guidance and may provide detailed procedures. Standard audit programs ensure certain elements of internal audit's methodology are considered or performed, and required templates such as a risk control matrix, audit report, and management self-identified issues assessment, help ensure consistent application of the methodology.

All documents, including the internal audit charter, are revised, as needed,

with updates identified through the QAIP process; new IIA, regulatory, or industry requirements; or requests for additional guidance from the audit teams. Documents are reviewed at least annually to identify required changes.

ONGOING MONITORING

Ongoing monitoring is achieved through continuous monitoring activities,

Customer surveys obtain feedback through scoring rather than comments to facilitate more efficient completion by business unit management.

including engagement supervision and feedback, internal audit management reporting, and internal QA reviews of audit and issue follow-up activity.

Engagement Supervision and Feedback

In addition to the requirement that all internal audit workpapers have a second level of review, the department has formally documented the required minimum level of review for all audit activity in a matrix that audit staff can easily refer to.

Customer surveys are sent to business leads for all engagements. Surveys have recently been updated to obtain feedback through scoring (poor, fair, good, very good, excellent) rather than comments to facilitate more efficient completion by business unit management and to support reporting on results. Internal audit initially used an external survey site, but it is working to bring surveys in-house to avoid any future security concerns with an external site. The results of the surveys are not reported to the audit committee or senior management, but are used to identify opportunities to improve the



audit process or to identify additional training needs.

Formal engagement evaluations are performed for all audit staff spending more than 80 hours on an engagement. This form also was changed recently to be score-based to increase efficiency in completion of the form (meets expectations, does not meet expectations, exceeds expectations).

as it requires additional preparation time and a more detailed review than an automated report. To support the ability to add additional reports, internal audit has changed the production cycle for certain reports from monthly to quarterly. Moreover, internal audit management reports are leveraged for audit committee reporting, with the audit committee receiving certain audit management reports annually (e.g., innovation and capability reports) or bi-monthly (e.g., quality reports).

Reviews provide the external auditors additional assurance on the effectiveness of the internal audit department as an entity-level control.

To ensure consistent performance, internal audit requires customer surveys and engagement evaluations for each engagement. These tools are an integral part of the audit process.

Internal Audit Management

Reporting This reporting is prepared and distributed monthly via a PowerPoint presentation to the CAE and audit leadership. The reports are in a dashboard format, with department averages for comparison. Metrics include:

- *Quality:* A year-to-date cumulative average score of all audit and issue follow-up internal QA reviews.
- *Efficiency:* Average days between audit announcement and report issuance, audit plan completion, and staff use.
- *Innovation and Capability:* Staffing activity, tenure, percentage of certifications, highest degree obtained, average training hours per auditor, and budget to actual comparison.

Additional planned reports include tracking of audit issue follow-up completion. Reports currently are prepared manually, which can be challenging,

Internal QA Reviews These reviews have two primary components: audit QA reviews and internal audit issue follow-up QA reviews. The audit QA reviews are cosourced with an external third party to leverage their subject matter expertise and knowledge of best practices. The reviews have contributed to the improved interaction with management as they promote consistent application of the audit methodology and process. Additionally, the reviews provide the external auditors additional assurance on the effectiveness of the internal audit department as an entity-level control. The reviews are performed throughout the year, independent of the periodic self-assessment process.

The professional practices team selects audits to be reviewed by the third party at the beginning of the year, and required templates include a QA checklist. Approximately 25 percent of current-year projects are selected for review. The QA checklist:

- Is broken down by phase (e.g., plan, fieldwork, report) and further broken down within each phase by key activity (e.g., announcement, risk identification, and walk-throughs in the planning phase).
- Includes specific criteria for each activity. Each section receives a score, which is totaled to derive an overall score (0 to 100) for the project. The scores are broken

50% of internal audit departments have implemented the periodic internal self-assessments component of the QAIP, according to the CBOK 2015 Global Internal Audit Practitioner Survey.

down between quality (60 percent) and documentation (40 percent).

Internal audit performs audit issue follow-up (AIF) reviews using a checklist similar to the engagement review checklist, but the focus is on AIF activities. Reviews are done quarterly on a sample of the past quarter's follow-up activity.

At the conclusion of engagement or AIF QA reviews, the QA checklist, including review comments, is shared with the responsible audit team members for their review. QA "lessons learned" are shared with the CAE, leadership team, and audit staff quarterly, and key observations are incorporated into training materials for future use, or methodology documents are updated to provide additional guidance as necessary.

Periodic Self-assessment Internal audit has recently put in place a self-assessment process to ensure it stays current with the *Standards*. Internal audit completes self-assessments in those years when an external assessment is not performed. In addition to interviews and surveys of stakeholder groups and review of internal audit activity, internal audit uses checklists developed based on QAIP guidelines promulgated by The IIA. The results of the internal QA reviews are leveraged for the workpaper quality review component.

Audit Committee and Executive Management Reporting Audit committee and executive management reporting are the most time intensive nonaudit-related element of the QAIP. To maximize efficiency in preparation of these reports, they are automated, where possible, and audit committee reporting is leveraged for executive management reports.

Audit committee reporting includes materials for the CAE's report to the audit committee at each board meeting, and a memo providing key updates during months when the audit

committee does not meet. The report includes regular categories:

- Current internal audit results.
- Internal audit issue and issue theme trending.
- Analysis of report ratings year over year. Internal audit has three report ratings: The control rating (satisfactory, needs improvement, unsatisfactory), a management awareness rating (high, medium, low), and a control environment trending rating (improving, unchanged, declining).
- An update on the status of the internal audit plan.
- An update on the department's methodology and QAIP results.
- A summary of headcount and staffing activity.

Quarterly, internal audit issues a dashboard to each business head with the status of internal audit activity in his or her area. The goal is to provide the executive with a view of what is reported to the audit committee, as it applies to his or her area. The dashboard includes a five-quarter trend analysis of the following for internal audit issues, Sarbanes-Oxley deficiencies, and matters requiring attention:

- Current inventory of issues by priority.
- Issue status change.
- Management self-identified issue percentage year-to-date.
- Remediation time frames.
- Internal audit ratings year-to-date.

Detailed issue status reports also are provided to the business monthly. These reports include issue description, priority, and status.


STRATEGIC PLAN

Internal audit's strategic plan is updated semi-annually. The first part of the plan outlines at a high level the department's vision, mission, and core values as well as four to five strategic areas of focus. The second part includes details

related to the department's strategic goals and action plans, including specific action items that will contribute toward achieving the goal and a target date for each action item. The goals and action plans span one to two years (a three-year horizon is recommended; however, Fannie Mae Internal Audit found two years to be more practical). Twice a year, the leadership team reviews the plan and status of the action items, adds new goals and action items as necessary, and changes time lines, if necessary. The plan and status against each goal is shared with internal audit management and the internal audit department at least annually.

QAIP EVOLUTION

While maintaining and continually refining the QAIP is challenging from a resource perspective, internal audit has found that its interaction with management and the audit committee has improved as a result of the refinements. For example, during the 2010 EQA, management noted opportunities for improvement in interactions with internal audit. No such feedback was received in the 2014 assessment, and IIA Quality Services noted that interviews with management indicated internal audit's role is highly valued.

Fannie Mae's QAIP continues to evolve with changes in the industry, leadership, and the regulatory landscape. In maintaining or making improvements to the program, the function must evaluate trade-offs between activities to ensure it does not spread itself too thin and lose the very benefits it is trying to reap. Internal audit also must consider which activities can serve multiple purposes, to maximize its time and resources. 

MARGARET ULVI, CPA, is chief of staff to the CAE and leads the Internal Audit Professional Practices team at Fannie Mae in Washington, D.C.



Citi Internal Audit undertook an ambitious project to transform its training and development, enhance consistency, and better meet stakeholder needs.

a strong foundation

Mark Carawan

A large, high-performance organization like Citigroup must have top-notch internal auditors, professionals who command both the technical skills to conduct complex audits and manage expansive portfolios—as well as the “soft” skills to present their findings in a professional, respectful, and effective manner. For internal audit to play its important role in maintaining Citi’s global leadership position, the company’s internal auditors must demonstrate skills that translate—seamlessly—across divisions and geographies. While the local market conditions and business practices may vary, we must be functionally the same and execute flawlessly whether in Chile or Taiwan.

Citi currently maintains internal audit teams in roughly 90 locations, based in more than 60 jurisdictions and covering over 100 countries. This deployment model is designed so that Citi’s internal auditors are closer to the businesses and regions they evaluate, enabling them to better understand the local regulatory environment and business context. In the recent past, Citi Internal Audit operated in just over a dozen locations. However, following a board decision to anticipate and meet emerging regulatory expectations, the audit function undertook a far-reaching transformation. In just over three years, Citi Internal Audit has increased its manpower from about 610 practitioners to today’s more than 2,000 on-the-ground personnel. The transformation was characterized not

just by growth, but also by dramatic changes to how we operate, and how we develop our people.

To effectively serve Citi's vast array of stakeholders across the group's broad geographical reach, internal audit must demonstrate consistency. Global effectiveness in internal audit requires a common taxonomy, a consistently applied methodology, standard management information and reporting, and impactful ways of communicating to stakeholders worldwide.

This year Citi Internal Audit launched the Citi Internal Audit Foundation Academy to reinforce and ensure effective maintenance of these common standards. The Academy is

interactions with local management and regulators, to how we execute our assurance plan and work together within the internal audit function.

AUDIT TRANSFORMATION

The Foundation Academy, and several other changes, grew out of the recent financial crisis. In the aftermath of the crisis, many boards and audit committees—including Citi's—closely examined and raised expectations for the internal audit function. To realize these expectations, we underwent a wide-ranging transformation, including increasing staff and further developing our methodology and training. We called it the Citi Internal Audit Transformation Initiative.

The initiative began in 2012 and formally concluded in December 2014. It involved 10 specific work streams, covering areas such as organizational design, resources, people development, audit methodology, and communications. We also established a Leadership and Development Committee for internal audit that oversees the training program and reports its findings and proposals to my Operating Committee, or IA OpCo (see "The IA OpCo Team" on page 41).

After establishing the IA OpCo, we then assembled a focus group to evaluate certain topics. For example, we wanted to assess the various types of professional tools, skills, and materials that internal audit professionals need—or could most benefit from—in their first 90 days with the organization, their first 180 days, their first two years, and so on. The focus group then developed specific recommendations, and we endeavored to determine the right kind of training programs to serve as an initial stage foundation for the educational requirements of the Chartered Member of the Institute of Internal Auditors (CMIIA) designation in the U.K. and The IIA's global Certified Internal Auditor.

The Citi Internal Audit Foundation Academy is meant to provide basic training for internal auditors.

a training program designed to ensure that an internal auditor in Mexico and a colleague in Singapore can cover the same business activity in each of these jurisdictions, and evaluate and report on that business area using a consistent approach, evaluation mechanism, and documentation while operating under dramatically different regulations and business environments. The language, rating, and escalation mechanisms are identical, allowing for standardized reporting and consistent communication to all stakeholders. Just as the military operates boot camp for basic training to get personnel ready for action and to perform in accordance with a standard set of requirements, the Academy is meant to provide basic training from an internal audit perspective—to provide Citi's internal audit professionals with a foundational understanding of expectations—from



Throughout this process, we were looking at the audit skills our professionals need—both for their current roles and as they progress within the organization. We established a proposed curriculum for the Foundation Academy and worked with the Chartered Institute of Internal Auditors (CIIA)—the professional association for internal auditors in the U.K. and Ireland—to refine that curriculum so it met our expectations and theirs. The program has since been accredited by the CIIA. Now, employees who go through the Academy’s training regimen receive the CIIA’s Certificate in Internal Audit and Business Risk designation as well. The process also saw the introduction of a Certified Internal Auditor program, launched at the beginning of 2015, and we are now making plans to adjust the program to embrace The IIA’s Certified Financial Services Auditor program.

THE RIGHT SKILLS

In creating the Academy’s training programs, we emphasized the ability of Citi’s internal auditors to provide effective challenge to senior management and demonstrate evidence in support of that challenge to the Board of Directors. While we focused on sharpening the traditional audit skills, we also placed importance on other areas. Among the key attributes of Academy training are:

- ➔ *Presentation skills.* We must ensure that our people can present their audit findings to senior management and the Board, so we offer training in report writing, among other communication skills.
- ➔ *Negotiation.* Internal auditors must have the ability to work effectively with senior management. If done correctly, management will understand and agree with the facts, the required actions, timeliness, accountability, and risk-based severity in Internal Audit’s conclusions. That is much

THE IA OPCO TEAM

The Citi Internal Audit Operating Committee (IA OpCo) comprises the function’s lead chief auditors by broad product area (Institutional and Consumer), key functions (Risk, Compliance, Technology—the latter including Change and Third-party Management), Treasury and Finance (including other corporate functions), and geography (Asia; Europe, Middle East, Africa; Latin America; North America, as well as Japan and Mexico). A key position in IA OpCo is the chief auditor for Citibank, as is the only practicing lawyer in Citi not reporting to the group’s general counsel—Internal Audit’s own general counsel. Also on the IA OpCo are the internal audit function’s human resources (HR) director—a member of the HR function, the internal audit communications officer, and the function’s chief operating officer (COO). Additionally, the committee includes the quality assurance chief auditor, who owns the methodology and assurance strategy, and who together with the COO, is essential to driving change and innovation.

more effective than delivering a finding and saying, “Fix it.”

- ➔ *Staff management skills.* Our internal audit leaders need to further cultivate skills in managing their staff, particularly as it relates to delivering performance evaluations, but also in how to motivate and develop team members, and drive the right culture. It’s easy to tell someone he or she is doing well; it’s not as easy to tell that person he or she isn’t doing well. Our people managers need to deliver constructive feedback in a way that positively impacts the individual, and provides the right outcome overall—for the individual and for Citi.

Indeed, we have found it is fundamental to train people to deliver tough messages, which is always a part of an internal auditor’s role. The Academy gives our staff the confidence and ability to do this effectively. It is a key part of what we do, and one of the ways we focus on it in the Academy is through role-playing, with senior professionals using firsthand experiences to train Academy students.

While overhauling the training programs and establishing the



A Certified Auditor's
THINGS TO DO

1. Invest In
Myself

2. Drive My
Career

3. Plan for
2016!!

Calling All Certified Auditors. Earn and Report Your CPE Credits.

Dec. 31 is just around the corner. Don't let the end-of-year rush sneak up on you when it comes to earning and reporting your CPE credits.

Comply with your CPE requirements and continue enjoying the benefits of your certified status. IIA members in North America receive free CPE reporting as a member benefit.*

* If you are not a North America IIA member, please check with your local institute for CPE reporting pricing.

Follow our handy guide at
www.theiia.org/goto/CPEOptions.

54% of internal audit **training** programs offered by employers include business knowledge related to the organization's industry, according to the CBOK 2015 Global Internal Audit Practitioner Survey.

Academy, our goal was to teach essential skills and identify areas for further engagement and evaluation. We intentionally created programs that allow our auditors to become familiar with Citi's risk governance framework, including the expectation to establish a high standard for a culture of compliance and control. While it was not designed to be a comprehensive curriculum, we are constantly seeking ways to enhance training for our talented professionals.

At the Academy, internal audit's Quality Assurance team teaches the internal audit overview and audit methodology coursework, plus additional core elements of the syllabus. That 9-to-5 training is conducted face to face, while we use computer-based training for some supplemental topics outside the classroom sessions, including internal audit data analytics. The in-person elements of the nine-month training regimen are offered at multiple regional locations throughout the world.

Some of the online coursework titles include: "Technology and Systems Processes Audit Coverage—Guidance Training," "Third Parties Audit Coverage," and "Introduction to Internal Audit—Finance." We're also in the process of developing several online modules into a two-day, face-to-face course for fall 2015, covering topics such as decision making, conflict resolution, problem solving, and building trust. The modules will be interactive, incorporating role-playing case studies.

A COMMON LANGUAGE

Of course, no effort as comprehensive as our internal auditor training development is without challenges. The biggest challenge thus far has been the widely deployed and diverse nature of our internal audit staff. While all of Citi's internal auditors speak English, more than half the staff is composed of practitioners for whom English is not


a first language. Accordingly, we are enhancing the program to cover a wide range of topics for our people in nearly 100 locations, in more than 20 languages. Whether an auditor's first language is Turkish or Mandarin Chinese, for example, the internal audit report needs to be delivered in English—yet local regulations, and the practicalities of follow-up and important local stakeholder communications, will likely demand that our internal auditor's local interaction will be in a different language.

WHAT'S NEXT?

The results so far are exactly as we envisioned. Academy training begins for new hires within the first 30 to 60 days,

As people progress, they are offered more comprehensive training to refine leadership and management skills.

and the curriculum and methodology enable our new hires quickly to operate effectively within Citi.

We are pushing ahead to focus on establishing a next-stage Academy to empower our more seasoned internal auditors to continue to progress and flourish. We want to foster the development of our internal auditors so that they can become managers, the head of audit for a particular program or geography, and as soon as they can develop, chief auditors responsible for a broad program of assurance. As people progress, they are offered more comprehensive training to further refine leadership and management skills to become the next generation of leaders—not only for the internal audit function, but for Citi overall. 

MARK CARAWAN, PHD, based in New York, is chief auditor at Citigroup.



Audit Management Software

	2006	2015
CUSTOMERS	25 users	25,000+ users
VERSION	2.0	10.0
REPLACEMENT OF TRADITIONAL SYSTEMS	0	70+ countries
OUTBOUND SALES CALLS	0	0

How has MKinsight™ become
the fastest growing
Audit Management Software
worldwide without making
a single outbound sales call?

+1 847 418 3898
www.mkinsight.com

Trusted by Companies, Governments and Individuals Worldwide.

BUDGETING FOR ANALYTICS

Using a systematic, sustainable mechanism to determine level of effort can help auditors develop a reliable analytics budget.

Data analytics tools are nearly ubiquitous in today's high-performance audit functions, with most either developing their analytics capabilities or increasing its use. And while the technology offers significant capabilities for audit enhancement, its value hinges on the users' ability to put analytics tools into practice and effectively plan analytics engagements. Accordingly, one of the most important steps in implementing a data analytics program is estimating the level of effort required.

Determining the right level of effort for data analytics at each engagement can be difficult, and its consequences immediate—including flawed analytics strategies and testing outlines. Some audit shops may systematically set aside a given percentage of the engagement budget for the use of data analytics. This approach is suitable for repeated audits or when the audit department has observed resource usage trends over several years. But because the objectives and scope of some engagements can be unique, requiring specific sets of testing

Rigobert Pinga Pinga

hypotheses and data sources, developing a systematic and sustainable mechanism for determining level of effort can result in a reasonable and justifiable budget for data analytics.

At the author's organization, tackling analytics budgeting involved three main steps: obtaining audit leadership support for analytics, crafting

by using a flagging system to identify potential candidates for data analytics. The list of flagged engagements can then be used to prioritize analytics work for effort estimation. The analytics team should also adopt a methodology to assess the likelihood and intensity of data analytics activities, as well as develop a level-of-effort matrix.

- Are the data needed internal or external to the organization?
- Does access to the data needed require additional effort and approval?

For experienced, data savvy auditors, brainstorming sessions can be a useful tool for high-level consideration of potential data needs and sources. The exercise can also facilitate development of detailed testing hypotheses and help define testing limitations. Early identification of data needed and the sources of that data can help shape data access negotiations with the IT team or the data owners.

Obtaining internal audit leadership support for analytics use is critical.

and following a methodology for determining analytics effort, and considering several critical success factors. Although the audit universe will vary from one setting to the next, and no methodology provides a one-size-fits-all approach, focusing on these three areas can provide a helpful foundation for those looking to enhance their analytics efforts.

LEADERSHIP SUPPORT

Obtaining internal audit leadership support is critical, as it sets the tone at the top for the effort and helps ensure a strong commitment to the use of data analytics on engagements. The CAE ideally should indicate his or her support for analytics use before the start of the annual risk assessment and audit plan development process. When communicating to staff, the CAE needs to explain the data analytics strategy and stress the need to allocate sufficient staff time at the engagement level. The CAE's open support will also reinforce budget accountability and trigger awareness and staff buy-in for the analytics budgeting process.

ESTIMATE LEVEL OF EFFORT

To determine level of effort, the auditors and data analytics team can begin

Identify Potential Candidates During audit plan development, internal audit managers should encourage their staff members to be mindful of analytics needs and to flag potential candidates for application of the technology. Because they know the organization's business processes, auditors should be at the forefront of identifying engagements that may require the use of analytics and determining how it can be best deployed to support audit results. They should also consider challenges that may be encountered on each engagement. Basic questions that auditors can ask themselves include:

- Can the audit team use data to support potential findings?
- Is the entity under consideration for review being monitored through the use of key performance indicators (KPIs)? What are those KPIs? What are the underlying data?
- What are the quick data analytics wins if the audit/review were to be conducted?
- Considering the objectives and scope of the engagements, what are the two or three broad testing hypotheses that can be formulated?

Assess Likelihood Once flagging is complete, the auditors and data analytics team can assess the likelihood of analytics activity for each engagement. A three-tiered assessment system can be applied:

- *None.* The engagement will not involve any data analytics activities, as its focus, objectives, and scope suggest that analytics will not be required. Reviews of process design or frameworks may fall into this category.
- *Likely.* The engagement may involve some data analytics activities. The analytics and audit teams anticipate that analytics work will be carried out—they have identified broad preliminary objectives and scope but cannot confirm them before the start of the engagement.
- *Certain.* The analytics and audit teams have determined the need for analytics, and the objectives and scope of the engagement provide strong indication that analytics work will be carried out. The auditors have identified a preliminary data analytics scope and comprehensive testing hypotheses. Some gray areas might appear, as likelihood assessments are not always

More than **50%** of internal auditors globally use data mining or data **analytics** to detect fraud, according to The IIA Research Foundation report, *Staying a Step Ahead: Internal Audit's Use of Technology*.

clear-cut. For example, at the time of audit plan development, the audit staff might not have enough information to decide whether or not data analytics activities will be carried out for some engagements. Or, the team may determine that analytics objectives and scope will be defined during engagement planning. Engagements with these characteristics should be kept in mind, and a contingent budget should be set aside to cover them should the need for analytics work arise.

In other circumstances, the delineation between Likely and Certain might not be sharply defined. When this occurs, a hybrid assessment can be used—None/Certain, None/Likely, or simply Yes/No.

Estimate Intensity Analytics intensity measures the degree to which analytics activities will be carried out in the selected engagements. The level of intensity can be measured using a low-medium-high scale:

- ➔ **Low:** Basic analysis is expected to be performed, and analytics resource usage is estimated to be low. The analysis may include profiling and pattern identification, as well stratification, gap analysis, and calculation of statistical parameters to identify outliers. Factors to consider when assessing the intensity as Low may include whether there are few data sources and if data are readily available.
- ➔ **Medium:** Data analytics activities include profiling and pattern identification, stratification, gap analysis, efficiency measurement, benchmarking, and calculation of statistical parameters to identify outliers. Factors to consider when assessing the intensity as Medium may include whether data needed is external to the

LEVEL-OF-EFFORT MATRIX

		Intensity		
		Low	Medium	High
Likelihood	Certain			Engagement E2
	Likely	Engagement E1		

organization, whether the analytics team will make additional effort to gather the internal data needed, and whether the analytics team anticipates that it will join several data sources in different systems to identify inappropriate matching values.

- ➔ **High:** The engagement is considered to be heavily data-driven, or analytics is the core of the review. Analytics activities include profiling and pattern identification, stratification, gap analysis, efficiency measurement, benchmarking, data sequencing, and calculation of statistical parameters to identify outliers. Additionally, the analytics and audit teams are expected to develop complex analysis and hypotheses. Factors to consider when assessing the intensity as High may include whether any data needed is external to the organization and if the analytics team will make additional effort to gather the internal data needed.

Develop a Matrix Using the likelihood and intensity data gathered, the analytics and internal audit team can create a level-of-effort matrix to help determine analytics budget estimates. The matrix should capture the thought



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

DATA ANALYTICS BUDGET FUNDING

	Engagement Name	Engagement Budget Basis (in days)	Data Analytics Budget as a Percentage of Engagement Budget	Data Analytics Budget (in days)	Total Engagement Budget (in days)
Scenario 1	Engagement E1	100	10%	10	100
Scenario 2	Engagement E2	100	20%	20	120

process for assessing the level of data analytics activities.

“Level-of-effort Matrix” on page 47 depicts an example matrix, showing the extent of data analytics activities at the engagement level. The dark tan color indicates that heavy analytics activities will be carried out in the engagements that fall into that category. For example, Engagement E2, with a likelihood of Certain and High intensity, will receive the highest percentage of the engagement’s total budget—say, 50 percent. Engagement E1, in which likelihood and intensity are assessed as Likely and Low, respectively, will receive a percentage significantly lower than that of Engagement E2—perhaps 10 percent. Engagements with likelihood assessed as None will receive no budget allocation for analytics activities. The analytics team should set percentages using professional judgment, taking into consideration trends observed in the past.

KEY SUCCESS FACTORS

To ensure an adequate level-of-effort estimation, the analytics team should view the budgeting exercise as a dynamic, multidimensional activity that takes into account some additional elements. Specifically, success factors for the continuous improvement of the data analytics level of effort include validation of the analytics budget, adoption of a

mechanism for funding the budget, and variance measurement.

Validation Process Although analytics level-of-effort estimation is primarily the analytics team’s responsibility, team members should work closely with internal audit. During level-of-effort formulation, the analytics team should ensure critical inputs are considered, including minutes of relevant audit staff brainstorming sessions, audit clients’ feedback on the proposed audit plan, and, if available, analytics usage trends observed during prior years.

The analytics team should constantly seek feedback from internal audit staff and management to ensure the assumptions and measurement indicators are well-understood. After applying the matrix, the team should conduct validation meetings with stakeholders, which may result in changes to the level of effort for each engagement.

The analytics team should record both calculated and adjusted levels of effort and document significant changes. This documentation is critical, as it can help refine the criteria for assessing likelihood and intensity of data analytics activities for subsequent years.

Funding Mechanism Because data analytics can increase engagement efficiency, support for a specific analytics budget should be clearly communicated across the entire audit department. Before

sharing the finalized budget, however, the department must first decide whether to increase the original budget for the engagement by the analytics budget or to make the analytics budget part of the original engagement budget. “Data Analytics Budget Funding” on this page depicts each of these scenarios.

In Scenario 2, the general budget of Engagement E2 is increased by 20 days, which corresponds to the data analytics level of effort. This scenario suggests that the analytics budget comes out of a central contingency envelope. By nature, this practice might defeat any efficiencies gain through the analytics work.

In Scenario 1, Engagement E1 has an unchanged general budget. This scenario reflects the notion of “doing more with less” on an individual engagement. Moreover, it generates a high perception of accountability among the data analytics and audit teams.

Variance Measurement After each engagement or at year-end, the analytics team should compare the initial or adjusted budget with the actual days spent. Any variances observed can help gauge the quality of level-of-effort matrix estimates. Low variances may indicate that empirical assessment was effective, whereas high variances might be an indicator that the criteria for assessing effort need some refinement. When budget overruns occur, the


analytics team should consider two important factors:

- ➔ **Experience Level.** If the data analytics team is too inexperienced, substantial deviations from the initial budget can be expected. But as the team gains more experience, deviations caused by this factor should decrease.
- ➔ **Analytics Process Maturity.** In early years of data analytics use, level of effort can be significant. Factors that may contribute to budget overruns include absence of a strong partnership/relationship with data owners or the IT department, absence of a clear process for identifying data needed, poor quality assurance surrounding the data analytics activities, absence of a robust infrastructure that supports

the analytics team's work, and poor quality of interactions between the analytics and audit teams.

BENEFITS AND BOTTOM LINE

Upfront identification of engagements that lend themselves to data analytics is critical, and it can yield several benefits. First, not only does it help determine the level of effort required, but it also provides a high-level indication of the types of data needed for those engagements. That way, the data analytics team can engage the IT function or the data owners early enough to avoid the bottlenecks of late requests. Additionally, it can have a direct impact on the CAE's decision-making process by identifying the analytics skills needed as well as isolating areas where co-sourcing would be cost-effective.

Estimating data analytics level of effort for each engagement within the audit plan can be challenging—even daunting, especially if the assessment is performed during audit plan development. And while the matrix system yields a considerable amount of useful data for decision-making, professional judgment ultimately should be the cornerstone of the entire process. An auditor's knowledge and experience should guide decision-making, using the level-of-effort methodology as a means of informing and supporting conclusions. 

RIGOBERT PINGA PINGA, CIA, CPA, CFE, CGMA, is audit specialist and data analytics champion for the Internal Audit Vice Presidency of the World Bank Group in Washington, D.C.

IIA SmartBrief – Your Essential Connection to Internal Audit News

IIA SmartBrief provides a weekly snapshot of market news and issues affecting internal auditors and their stakeholders from leading global news sources.

This complimentary benefit of IIA membership offers a quick read that will keep you up to date on the latest news and trends in our industry.



Subscribe now at
www.smartbrief.com/iaa.

 **The Institute of
Internal Auditors**

141-093



Enhance the Health of Your CEO / CFO Certification Program

Are you comfortable that your SOX 404 or National Instrument 52-109 program:

1. Is cost-effective, pragmatic and focusing on high risk areas?
2. Improves your business processes and system of internal controls?
3. Aligns with the new COSO framework and other common industry practices?
4. Meets the rigour of a regulatory examination or external audit?
5. Provides an adequate due diligence defence if challenged in a court of law?

MNP has successfully assisted more than 80 public companies comply with SOX 404 and National Instrument 52-109 requirements.

How healthy is your CEO / CFO Certification program?

Gordon Chan, *National Enterprise Risk Services Leader*
gordon.chan@mnp.ca or 1.877.500.0792



Preserving the Organization's Moral Landscape

SERGEY NIVENS / SHUTTERSTOCK.COM



By assessing integrity and ethics safeguards, internal audit can help the organization protect against fraud and other wrongdoing.

Bruce Turner

“**G**ood business leaders should be a step ahead of what customers want ... and good auditors often need to be a step ahead of management,” asserts IIA–Singapore’s May 2014 report, *The Changing Role of IA: Keeping Watch for the Board*. Internal auditors can keep a step ahead of management by anticipating its need for an assessment of the organization’s integrity and ethics safeguards, and placing it high on the audit plan. This is appropriate, given that 87 percent of executives surveyed around the world consider reputation risk to be the most important strategic risk, according to Deloitte’s 2014 Global Survey of Reputation Risk. A reputation that has taken many years to build can be ruined quickly when incidents that diminish the organization’s moral landscape become public knowledge.

Organizations that have clearly articulated values and a strong culture of ethical behavior tend to control fraud more effectively. They usually have well-established frameworks, principles, rules, standards, and policies that encompass the 10 typical attributes of fraud control. These attributes include leadership, an ethical framework,

responsibility structures, a fraud control policy, prevention systems, fraud awareness, third-party management systems, notification systems, detection systems, and investigation systems.

Internal auditors need to sharpen their thinking when planning an assessment of their organization's integrity and ethics safeguards (Standard 2010) and then performing the engagement (Standard 2300). Conducting research across

their organization, industry, and region will help them determine the emerging risk areas and potential gaps in organizational safeguards. Four key elements of integrity and ethics safeguards have emerged over the past year related to fraud control planning, handling conflicts of interest, shaping ethical dealings with third parties, and natural justice principles for employees facing allegations of wrongdoing.

Fraud Control Plan

The need for a fraud control plan is borne out by an organization's potential fraud losses—typically about 5 percent of revenues are lost to fraud each year, according to the Association of Certified Fraud Examiners' 2014 Report to the Nations on Occupational Fraud and Abuse. A fraud control plan typically will articulate an organization's fraud risks, controls, and mitigation strategies, including:

- ➔ Significant business activities.
- ➔ Potential areas of fraud risk.
- ➔ Related fraud controls.
- ➔ Gaps in control coverage and assurance activities.
- ➔ Defined remedial actions to minimize fraud risks.
- ➔ Review mechanisms evaluating the effectiveness of fraud control strategies.

Management should review and update the fraud control plan periodically and report the results to the audit committee and senior management (see "The Coordinated Assessment" on this page). In organizations where internal audit is responsible for reviewing the fraud control plan, it should be performed by the CAE. This review should be integrated into the organization's wider business planning to ensure synergies exist with other areas, and it should illustrate the specific links to the organizationwide risk assessment and anti-fraud activities.

The Coordinated Assessment

A financial institution with a separate manufacturing arm was generating annual net profit of more than US\$4 billion through local and global operations (based on real cases). According to news reports, it was expanding its product sales into relatively unknown international markets. The audit committee recognized the organization's expanding fraud vulnerabilities through separate reports it was receiving on risk topics such as procurement shortcomings, organized criminals infiltrating the organization to gain access to confidential information, allegations of bribery of foreign officials through "facilitation payments," increasing incidents of cybercrime, and greater digital connectivity. Committee members asked the CAE to facilitate a coordinated organizationwide assessment of fraud vulnerabilities, with the results to be consolidated into a fraud control plan.

The CAE drew together knowledge experts from various business areas to identify potential fraud vulnerabilities. The group considered global research on reported and emerging fraud risk areas, then debated the strength and effectiveness of the organization's internal controls. Through workshop analysis, the group identified the highest risk areas of potential fraud and their three lines of defense, which included risk owners and management; risk control, compliance, and monitoring areas; and internal audit. In addition, the group noted opportunities to strengthen current fraud risk management arrangements.

The group consolidated the workshop outcomes into a fraud control plan, which was validated by senior management. The analysis also was used to update the organization's assurance map, which identified and mapped the assurance arrangements over key risk areas, business processes, and organizational objectives into a central record.

The CAE reported the results of the workshop together with the fraud control plan to the audit committee. The CEO assigned ownership of the fraud control plan and the associated actions to senior management and asked the CAE to confer with senior management to provide semi-annual progress reports to the audit committee.

22% of respondents say they have firsthand knowledge of workplace wrongdoing, according to a recent University of Notre Dame/Labaton Sucharow survey of financial service professionals.

Managing Conflicts of Interest

The Organisation for Economic Co-operation and Development reports, "There is a growing consensus that managing conflicts of interest is critical to curbing corruption." Reports indicate that unmanaged conflicts of interest continue to cost organizations millions of dollars. To minimize these risks, organizations need a clear and well-understood conflict of interest policy, coupled with practical arrangements to implement and monitor policy requirements (see "A Lack of Governance" on this page).

The U.K. National Audit Office defines a *conflict of interest* as a set of circumstances that creates a risk that an individual's ability to apply judgment or act in one role is, or could be, impaired, or influenced by a secondary interest. The perception of competing interests, impaired judgment, or undue influence also can be a conflict of interest.

Good practices for managing conflicts of interest involve both prevention and detection, such as:

- Promoting ethical standards through an explicit conflict of

- interest policy as well as well-stated values and clear conflicts provisions in the code of ethics.
- Identifying, understanding, and managing conflicts of interest through open and transparent communication to ensure that decision-making is efficient, transparent, and fair, and that everyone is aware of what to do if they suspect a conflict.
- Informing third parties of their responsibilities and the consequences of noncompliance through a statement of business ethics and formal contractual requirements.
- Ensuring transparency through well-established arrangements for

- declaring and registering gifts and other benefits.
- Ensuring that decisions are made independently, with evidence that staff and contractors routinely declare all actual, potential, and perceived conflicts of interests, involving at-risk areas such as procurement, management of contracts, human resources, decision-making, and governmental policy advice.
- Establishing management, internal controls, and independent oversight to detect breaches of policy and to respond appropriately to non-compliance.

A Lack of Governance

The XIX Commonwealth Games were held in Delhi, India, in 2010 and involved almost 6,500 athletes and officials representing 53 countries. India emerged successfully as both host and competitor, achieving many of the objectives of hosting the games, including large-scale improvements to city and sporting infrastructure.

Inexplicable delays in decision making put pressure on time lines leading up to the event and led to the creation of an artificial or consciously created sense of urgency. The target date was immovable and could only be overcome by obtaining waivers from government procedures. Many contracts were then entertained based on single bids, and some were even awarded on a nomination basis. There were perceptions that competing interests, impaired judgment, and undue influence had led to unmanaged conflicts of interest.

After the games, an independent report by India's comptroller and auditor general reflected that the games preparations adopted a governance model "in which authority was dissipated, accountability was defused, and unity of command was not provided for or followed." The report concluded that "eliminating (procurement) competition led to a huge extra burden on the exchequer." The comptroller and auditor general reflected that, "Taking liberties with governmental procedures ... led to elimination of competition. A conclusion from such action which seems obvious is that this could indeed have been an intended objective!" In the wake of the report, the BBC reported the chairman of the Commonwealth Games Committee was fired, arrested along with nine others, convicted of corruption, and jailed.

Good practices for managing conflicts of interest involve both prevention and detection.

Statements of Business Ethics

Contemporary business models increasingly involve third parties, with external supplier costs now representing one of the most significant lines of expenditure for many organizations. Such interactions can provide an opportunity for fraud and corruption (see “Improper Deposits” on this page).

The International Federation of Accountants and the Chartered Institute of Public Finance and Accounting recognize that “an entity’s strong commitment to ethical values needs to be communicated to suppliers through a Statement of Business Ethics,” according to their International Framework: Good Governance in the Public Sector, issued in July 2014.

Many forward-thinking organizations already have codes of ethics in place that set out the values and ethical expectations of both their board members and staff. The board code of conduct should define the behavioral standards for members, while the staff code of conduct should detail standards for employee conduct and the sanctions that apply for wrongdoing. Similar statements also are appropriate for third parties such as suppliers, service providers, and business partners.

A statement of business ethics outlines both acceptable and unacceptable practices in third-party dealings with an organization. Common features include:

- ➔ The CEO’s statement on the organization’s commitment to operating ethically.
- ➔ The organization’s values and business principles.
- ➔ What third parties can expect in their dealings with the

organization and the behaviors expected of them.

- ➔ Guidance related to bribery; gifts, benefits, hospitality, travel, and accommodation; conflicts of interest; confidentiality and privacy of information; ethical communications; secondary employment; and other expectations.
- ➔ Contact information for concerns, clarification, reporting of wrongdoing, and disputes.

Once established, the organization needs to implement a well-rounded communication strategy for the statement of business ethics that includes education of staff members, distribution to third parties, publication on the organization’s website, references to it in the annual report, and inclusion in future tender proposals and bid packs.



VISIT
[Internal Auditor.org](http://InternalAuditor.org)
for more
resources
on business
ethics.

A statement of business ethics outlines acceptable practices in third-party dealings.

Improper Deposits

The tendering manager at Integral Energy Australia, Dennis Hall, sought expressions of interest for decommissioned electrical transformers from his company’s panel of preferred purchasing tenderers. He and a colleague would usually accept the highest price offered.

The successful bidder was asked to pay the funds by check made payable to “Dennis Hall, the Administrator, Manager, and Trustee for the Scrap Process.” Hall would deposit the funds into his personal account and, if requested, provide a receipt on Integral Energy’s letterhead.

By the time the company discovered his activities after two and a half years, Hall had appropriated almost AU\$400,000 (US\$294,820). An independent investigation found his dishonest behavior included fraud, theft, embezzlement, forgery, and official misconduct.

Hall was subsequently convicted and sentenced to two and a half years in prison. In the wake of the discovery, Integral Energy strengthened its policies and procedures, and implemented a statement of business ethics detailing the way in which the company would interact with third parties that did business with it, including requirements for checks.



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

Charter of Rights

Engaged and capable employees underpin the success of most organizations, yet management does not always recognize the bottom-line effects and employee turnover costs when innocent employees are the subject of allegations of fraud and other wrongdoing (see “Guilty Until Proven Innocent?” on this page). About 60 percent of allegations against employees turn out to be unsubstantiated, according to the 2014 NAVEX Global Ethics and Compliance Hotline Benchmark Report.

A charter of rights compiles in a single document all of the information that respondents to allegations of wrongdoing may require. Such a charter should be written in an easy-to-understand style to meet the needs of its target audience. It should:

- ➔ Outline the charter’s purpose, how it will operate, how it supports a robust complaints and allegations system, and how it aligns with the organization’s values.
- ➔ Describe how management handles workplace allegations and complaints, and ensure principles of natural justice and other legislative obligations, such as privacy, are in place.
- ➔ Provide a high-level overview diagram of the allegation assessment and investigation process, including the channels for submitting allegations; the distinct phases for logging, assessing, and investigating the allegations; and the final decision-making phase.
- ➔ Include details of available support such as contact information for human resource specialists, details about an external confidential employee help line, and processes for updates throughout the investigation.
- ➔ Illustrate the tiered escalation process for handling allegations that reflects (at one end) how issues of a serious, sensitive, or significant nature are addressed, and encourages (at the other end) the handling of low-level localized issues as close to the source as possible.
- ➔ Provide answers to common questions that respondents might have about the process for dealing with allegations, such as “What can I expect?” “Are outcomes always reviewable?” “What does frivolous and vexatious mean?” “What will I be told about the outcome?” and “What happens when a process is concluded?”
- ➔ Outline the options for independent reviews of adverse investigation outcomes.

Guilty Until Proven Innocent?

Ron White had reached the pinnacle of his career when he was recruited to lead a specialist governance function in a large public sector organization that had total annual expenses of more than US\$3 billion. (This story is based on a real case, but White’s name has been changed.) After he had been with the organization for a few months, allegations of inappropriate behavior were raised against White. Although he was subsequently proven innocent, the allegations were of such a serious nature that they could potentially derail his career.

The organization had many policies and procedures covering ethics, allegations, and investigation approaches, but White had difficulty locating all the information he needed to fight the allegations. That information was virtually nonexistent or seemed hidden among other corporate policies, as if it were an afterthought.

Based on his experience, White realized that alleged perpetrators needed some help, through a charter of rights. He broached the idea with the CEO and gained his support. The legal team recognized the natural justice value of having a charter of rights to provide just, fair, and reasonable resources for the organization’s staff. Moreover, the availability and dissemination of these resources could be demonstrated to the courts in the event of a lawsuit against the organization. The executive leadership team was tasked with developing a charter of rights, and did so through a wide consultation process involving staff representatives, lawyers, investigators, the CAE, trade unions, and other stakeholders.

A STEP IN THE RIGHT DIRECTION

Many of the resources produced for the public sector on integrity and ethics safeguards can be adopted for the private and not-for-profit sectors, where similar resources may not be available. The IIA Research Foundation’s 2015 report, *Driving Success in a Changing World — 10 Imperatives for Internal Audit*, reflects the importance for internal auditors to anticipate the needs of stakeholders. This is consistent with the core principle for internal auditors to be insightful, proactive, and future-focused. Placing an assessment of the organization’s integrity and ethics safeguards high on the audit plan is a step in the right direction. [la](#)

BRUCE TURNER, AM, CRMA, CISA, CFE, is the audit and risk committee chairman of IIA-Australia.

The *Effective* CAE

Norman Marks

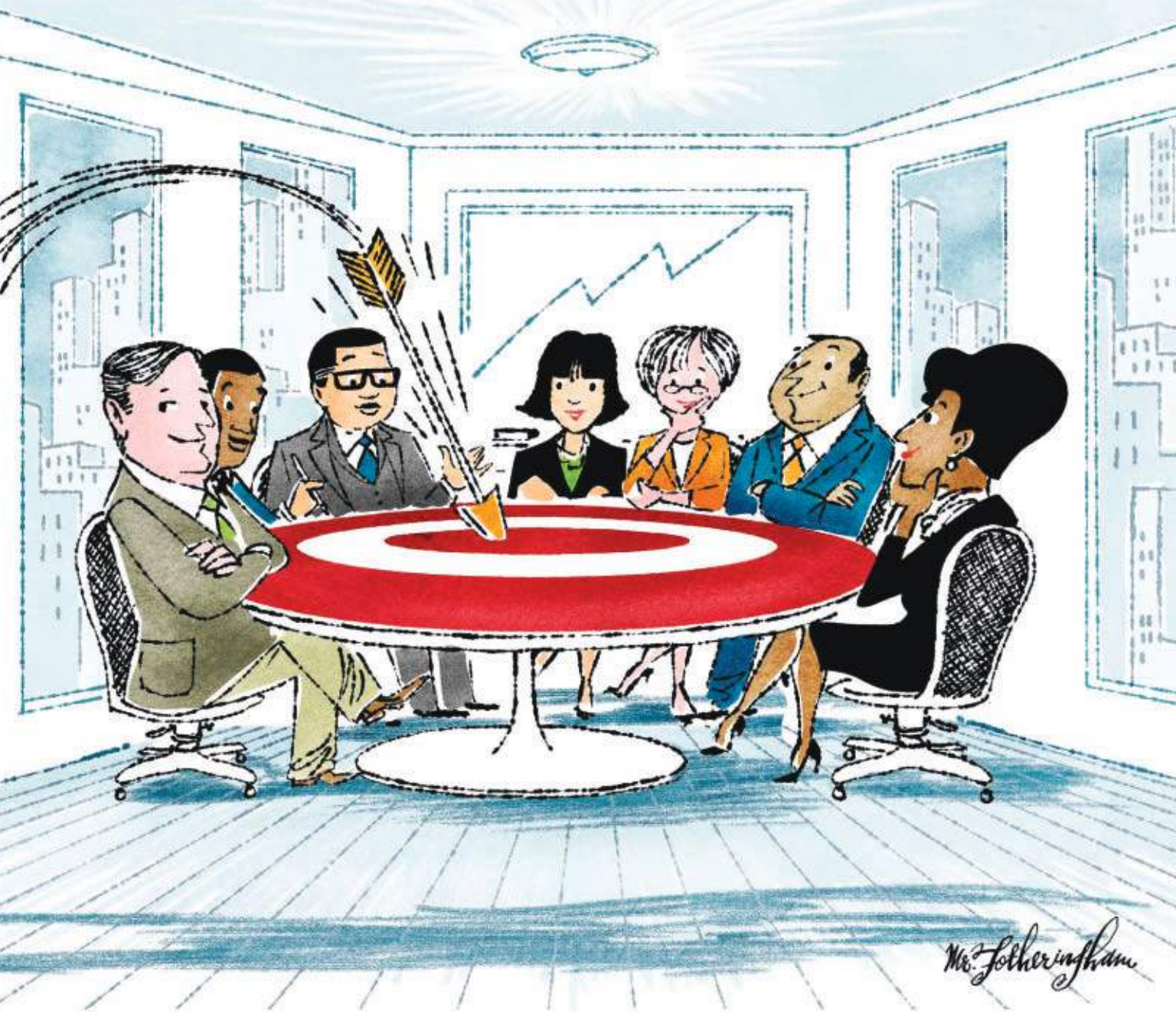
Illustration by Edwin Fotheringham



Adaptable CAEs who look to make changes in how internal audit addresses critical risks are the biggest benefit to stakeholders.

The world in which we live and work continues to change at an accelerating pace. As it changes, CAEs need to constantly ask whether they should make changes to their practices. The fact that something has been seen as successful in the past, even when stakeholders applaud the value it has contributed, does not mean complacency should follow.

According to KPMG's 2015 Global Audit Committee Survey, only 40 percent of audit committee members are satisfied that internal audit delivers the value to the company it should, down from 45 percent in 2014.



Another 38 percent are somewhat satisfied. Moreover, a member of multiple boards in New Zealand wrote in an August 2015 blog post about his experience with internal audit functions, saying internal audit was focusing only on compliance and financial reporting, and that, “Almost all of [internal audit] findings are mundane operational compliance issues.”

Leading CAEs are adapting their practices and making contributions to the understanding of emerging and strategic risks; they also have a very broad remit from their audit committee. When it comes to internal audit

providing more value to the organization it serves, each CAE and his or her stakeholders need to decide what is needed for their organization — for some, an overhaul may be in the cards.

ENTERPRISE RISK-BASED AUDITING

In recent years, internal audit has moved from the traditional risk-based approach of building audit plans to addressing risks in processes and at locations (risks that matter to operating management) to auditing the critical risks to the organization referenced by KPMG (those that

matter to the board and top management) — enterprise risk-based auditing. This has meant leveraging the organization’s risk assessment (assuming management has an acceptable risk management system in place) to 1) understand the organization’s goals, objectives, and strategies for achieving them; 2) understand the related risks; and 3) provide assurance and advisory services that help the organization succeed by managing those risks effectively. The process involves not only sharing assurance and traditional recommendations, but also insights and ideas. It’s about recognizing that

there is little value in helping managers avoid the occasional stumble compared to the greater value of helping it take the right level of the right risks— risks to the corporate objectives. The board and top management view the internal audit department as making a positive contribution to success, not just helping them remain in compliance or make improvements in processes.

Years ago, the internal audit department rarely provided the board or top management with information that led the organization to change its strategies. The more advanced internal audit department of today focuses on issues that are critical to the success of the organization as a whole. Identified problems get the immediate attention of leadership because they represent obstacles or opportunities that matter to the board and executive team. Nowadays, the effective internal audit department rarely performs an audit where identified significant issues would not merit the prompt attention of leadership.

Today's internal audit department has moved from the outdated concept of basing its audit plan on an audit universe to basing it on a risk universe, with its eyes on the future rather than

HOW TO ALIGN THE AUDIT PLAN

- » Consider how the audit plan and the process for developing and maintaining it should be changed so that it includes, on a continuing basis, engagements designed to address the risks that matter to the success of the organization. What will be needed to ensure internal audit is aware of changes in risk, such that elements of the plan should be changed— audits added, changed, or removed—timely?
- » Discuss the extent to which the risk-based plan can leverage management's risk management system.
- » Determine how often the board and senior management will be updated on significant changes in the audit plan.
- » Obtain the approval of the board and senior management for the change, explaining how it will provide them timely information on issues relevant to the achievement of organizational goals and strategies.
- » Implement the change, paying special attention to communications within internal audit and with management across the organization.
- » Monitor the risk-based audit planning process by obtaining feedback from stakeholders on whether the engagement and its results were relevant to their management and oversight of the enterprise, and understand why the audit plan was not updated when risks changed and the plan did not.

The effective CAE has moved to update the audit plan almost continuously, at the speed of the business and the risks to its objectives. He or she is constantly listening to management and ensuring that every audit scope focuses on the risks of today and tomorrow.

The effective CAE updates the audit plan almost continuously, at the speed of the business.

the past. Its audit plan includes audits of risks that matter now and in the near-term, rather than the traditional audits of history. Internal audit is aligned with a board and executive team that is looking at how it can manage and lead the organization in the present and into the future.

While CAEs care deeply about being perceived as an objective provider of internal audit services, they also care about being considered as performing services that matter. Traditional barriers built to protect internal audit independence are challenged: Do they pose a threat to objectivity,



33% of CAEs report administratively to the chief financial officer and 29% to the CEO, according to The IIA Research Foundation's recent report, *The Evolving Role of the CAE*.

and do they inhibit the department from doing what is necessary for the organization to succeed? Barriers to value are torn down.

In fact, effective CAEs measure success, at least in part, through the success of the organization. CAEs know that by addressing critical risks to the organization's strategies and helping it seize opportunities as they arise, they are making a valuable contribution to that success.

WORKING WITH THE BOARD

The prevailing model has internal audit reporting functionally to the audit committee (or equivalent) and administratively to a senior officer. Board structures are changing and internal auditors are being asked to do more. Does it make sense to continue to limit internal audit to working with the audit committee, even one that has expanded beyond financial reporting and financial management to include oversight of the risk management?

For example, if there is a compliance committee, the effective CAE provides its members with the information they need on the condition of compliance-related processes and risks. If the organization establishes a risk committee to oversee management's processes for managing risks to the enterprise's objectives and strategies, the effective CAE participates in every meeting, just as he or she does with the audit committee.

TIMELY COMMUNICATION

Today's executives and managers receive information through dashboards, emails, and even text messages. Yet, most internal audit departments continue to send stakeholders long, written reports (at best, attached to emails) that make the reader find the time to absorb and understand the large amounts of information shared with them.

In fact, The IIA's *International Standards for the Professional Practice of Internal Auditing* does not require that an audit report be issued at the end of each engagement. Instead, it requires internal audit to communicate the results of its work.

The traditional audit report is several pages long, although on occasion it may resemble a small book with an executive summary. It is carefully crafted to express an opinion (usually) and influence management to make valuable changes in its business processes. Unfortunately, that careful crafting takes time and may delay the message to stakeholders.

If internal audit is focused on risks that matter, it is only logical that the sooner its assessment, insights, and suggestions for change are communicated, the better. But the traditional audit report, even if reduced to a one- or two-page executive summary, might take weeks or more to draft, discuss with lower levels of management, and then issue.

The effective CAE communicates at speed. He or she has taken the

STEPS TO WORKING WITH THE BOARD

- » Talk to the chair of the audit committee and others as appropriate, such as the lead independent director and the chairs of the governance, risk, and compliance committees.
- » Understand the value and possible issues should internal audit's functional reporting line change. Consider the option of reporting to the lead independent director, or to a combination of committees, such as audit, risk, and compliance. If a combination, who would take the lead when it comes to oversight of the internal audit function?
- » Consider the option of internal audit continuing to report functionally to the audit committee, but attending and providing periodic reports to other committees.
- » Consult with senior management, such as the CEO, chief financial officer, and board secretary, to obtain their opinions.
- » After agreement has been obtained with all interested parties, modify the internal audit and board committee charters as needed.

Where insights lead

Deloitte differs in how we help you deliver uncommon business insight through internal audit. How we seamlessly shape a tailored client experience through leading-edge technologies and methodologies. How we lead through innovation to deliver internal audit results with more accuracy, efficiency, and value. And most important, how we turn insight into foresight. Developing and delivering ideas that are focused not just on any tomorrow, but on your tomorrow.

Explore our latest thought leadership on internal audit's vital role in cybersecurity and strategies for building a sustainable data analytics function for internal audit.

See [where a new approach to internal audit can take you](#). See [where insights lead](#).

www.deloitte.com/us/internalaudit

Deloitte.



As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/ about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2015 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited



time to learn what stakeholders need to know. The CAE understands what is important for them to hear and doesn't waste their time with what is not. While the internal audit report was once considered a product, today's effective CAE sees the report as just one way to communicate. Instead of using the audit report to document the

to see much of what is traditionally included. They need to know:

- If there is anything to worry about, because it may impact critical business strategies and plans.
- If there is anything to do or monitor at their level because there is a risk that appropriate action may not be taken.

While sharing more with the busy executive or board member may be tempting, it is not necessary.

results of the audit and to tell the stakeholders what is important to internal audit, the CAE communicates what the stakeholders need to know. He or she recognizes that operating management has already been informed at the engagement closing meeting and senior management and the board don't need

While sharing more with the busy executive or board member may be tempting, it is not necessary. Today's CAEs know how busy they are, and that by respecting their time, when CAEs do share information with them, they are far more likely to pay attention. They know that the CAE will

ACTIONS FOR EFFECTIVE COMMUNICATION

- » Meet with internal audit's stakeholders at the board, executive, senior, and operating management level. Understand their needs for information: What do they need and when and how can it best be delivered and readily consumed? Explain the shift from an internal audit reporting process to a communications process.
- » Determine how to meet those varied needs, such that they receive all the information necessary (in their view) to their success—and no more—when they need it.
- » Consider a strategy where communications with operating management revolve around the audit closing meeting.
- » Understand when it is appropriate to delay communications with more senior management or the board until a formal audit report has been completed, and when it is necessary to communicate promptly.
- » Design a communications process that is efficient to prepare, easy to consume by the reader, actionable by management, and timely. This may require multiple levels of communications vehicles.
- » Before implementing any change, share the plan with all interested parties and obtain not only their feedback, but also their agreement.
- » Monitor the success of the change by meeting with stakeholders and determining whether the new communications meet their needs.

IIA Resource Exchanges

The most comprehensive and up-to-date list of resources for guidance, knowledge sharing, publications, certifications, training, events, and more.



Risk Resource Exchange

Today's business environment is characterized by mounting pressures for stronger, more effective risk management. The Risk Exchange provides useful tools and resources, including the latest news and developments on risk issues, creating a global forum for the aggregation and sharing of knowledge.



CBOK Resource Exchange

Access the latest reports and tools to support your efforts in validating and benchmarking trends and emerging issues based on the largest and most comprehensive ongoing study of the internal audit profession. More than 25 free reports will be released through 2015 and 2016.



COSO Resource Exchange

Access the latest news, resources, tools, knowledge sharing, and training to support your implementation efforts of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control–Integrated Framework* (2013) and *Enterprise Risk Management–Integrated Framework* (2004).



Audit Committee Resource Exchange

The critical connection between audit committee effectiveness and internal auditing mandates that committee members maintain an in-depth understanding of internal audit best practices and how their internal audit activity is functioning. Access tools and resources to manage your audit committee relationship more effectively.



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

only report what they want and need to know.

Conveying this information through a phone call, in a meeting, or even in a short email may sometimes be sufficient. Integrating time-critical information into an executive's routine for receiving updates may be even better. For example, can the results of an audit be included in the executive's daily dashboard, signaling, perhaps through an alert or red light, when there is an issue that needs his or her prompt attention?

To do this requires that the engagement closing meeting include commitments by operating management to act on agreed issues. If they are sufficiently important to discuss and management has agreed action is necessary, there is no need to wait until the recommendations are communicated formally.

The successful internal audit department recognizes that it and management have limited resources. Therefore, it avoids work that does not represent value to its primary customer—following Lean principles. That includes sharing what matters in a phone call rather than spending time on a long audit report.

By eliminating unnecessary work, the internal audit department can complete more audit engagements and deliver more valuable insights to leaders of the organization.

A COMPETITIVE ADVANTAGE

While I was CAE of Tosco Corp., the president of our largest division told a visiting politician that one of the reasons the company was succeeding was because internal audit gave him a competitive advantage. This was because internal audit gave him assurance that it focused its work on the risks that were critical to his division's success and that the company's business processes could be relied on to manage risks at

KEEPING THE COMPETITIVE ADVANTAGE

- » Meet with stakeholders regularly and ask them to assess whether they would pay for internal audit services – not that they are going to be asked to do so – because they help them to be more successful.
- » Never be satisfied with success. Continually challenge everybody in internal audit, as well as its stakeholders, to identify opportunities to improve – even if the existing model is working well.

acceptable levels. Where they needed improvement, audit worked with management to identify the appropriate corrective actions. The board agreed, knowing that audit's continuously updated audit plan would address the critical risks to the organization.

While the audit reports were streamlined, if I were still in the role of CAE, I would look to change them

are always looking to help executives and the organization succeed. It is only through these interactions that he or she will know what needs to change—and the cycle continues.

FULL POTENTIAL

When an internal audit function is able to provide the assurance and advisory services needed by the board

By eliminating unnecessary work, the internal audit department can complete more audit engagements.

today by working with the key executives to understand how they receive important information from their direct reports and how they monitor the state of their business. Where possible, I would integrate audit assessments into that information flow, supplemented by meetings or phone calls.

In this virtual, connected world, the value of face-to-face meetings has not diminished. Personal contact with stakeholders not only to communicate what they need to know and when they need to know it, but also to ensure a constructive conversation on internal audit's assessment and insights on the business, goes a long way. Successful CAEs, after all,

and executive team, helping them lead the organization to success, it is reaching its potential. The effective CAE streamlines the function to do more, faster. He or she not only addresses the issues critical to organizational success, but also communicates valuable information clearly and rapidly—at the speed of the business. The ability to get away from old, outdated thinking and processes and adapt to meet changing business priorities is the foundation of a successful internal audit department. [la](#)

NORMAN MARKS, CRMA, CPA, was a CAE at major global corporations for more than 20 years. His blog, "Marks on Governance," is on InternalAuditor.org.



Great news for IIA members!

If you're a member of the Institute of Internal Auditors, you could save even more on GEICO car insurance with a **special discount!**



GEICO[®]
#MemberDiscount

geico.com/acct/iaa | 1-800-368-2734

Some discounts, coverages, payment plans and features are not available in all states or all GEICO companies. Discount amount varies in some states. One group discount applicable per policy. Coverage is individual. In New York a premium reduction may be available. GEICO is a registered service mark of Government Employees Insurance Company, Washington, D.C. 20076; a Berkshire Hathaway Inc. subsidiary. GEICO Gecko image © 1999-2015. © 2015 GEICO

Governance Perspectives

BY ROB BLANCHARD + KEVIN O'SULLIVAN EDITED BY MARK BRINKLEY

BIG DATA RISK AND OPPORTUNITY

Having an action plan to address both can add tremendous value to the organization.

To an internal auditor, just the term *big data* can elicit a sinking feeling. The challenges associated with the volume, complexity, and variety of big data can be overwhelming. The good news is, with a solid action plan, internal auditors can do more than just mitigate the risks associated with big data. Internal audit also can help exploit big data to identify and mitigate existing risks.

Big data is the collection of data sets that are so large and complex that they are difficult to process using conventional database tools. Big data comes in two flavors: structured data (e.g., data in spreadsheets and databases) and unstructured data (e.g., social media posts, emails, audio, video, and GPS data). And, of course, big data can have multiple sources. Typically, working with big data requires new technologies to identify usable business insights, trends, and correlations—often in real time.

Businesses are using big data not only to boost performance, but also to reduce risks and prevent loss. From a risk management perspective, companies can identify risks and create value by using big data in three areas: business opportunities and risks, IT governance, and internal audit opportunities and risks.

First, business opportunities result from the fact that companies have valuable data but often don't know how to use it to gain actionable insights. Rules creation and testing, personalization of product offerings, using social media to spot consumer trends, and the ability to make data-driven business decisions all represent significant big data opportunities.

But these opportunities come with risk. For example, how does a company store personally identifiable information, and who owns it? How does it address regulatory issues and privacy breaches? What about increased exposure to reputa-

tion risk? And how should data retention, such as timing of disposals, be managed?

Big data considerations in the area of IT governance tend to focus on data-center management, specifically capacity planning and monitoring because of the massive replication of data at the software level and the need to measure performance. Of course, IT security is a tremendous concern, as are access control, penetration testing, and the quality of systems testing and processes.

Finally, internal audit opportunities and risks are centered around the security and compliance related to big data implementation, with issues such as ownership of data, authority to access, and secure access as priorities. Also, auditors exploit big data in the areas of continuous controls monitoring, access to nontraditional data sets, and regulatory compliance.

An organization's plan for addressing these three areas will vary according to its

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



Learn more at
www.theiia.org/goto/awareness



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

industry, goals, and challenges. However, there is a high-level, phased-action-plan approach any enterprise can customize:

- » Phase 1: Identify where data resides in the organization and the roles and responsibilities related to it.
- » Phase 2: Define goals and priorities.
- » Phase 3: Assess critical data issues.
- » Phase 4: Identify key risk indicators (KRIs).
- » Phase 5: Identify opportunities to add value.

By applying these phases to each of the three identified areas, internal auditors and risk management professionals can identify and mitigate big data risks and seize any opportunities.

An action plan for addressing IT governance, for example, should focus on the implementation team's responsibilities in phase 1, including security, capacity planning, code writing, pinpointing the owner of specifications, and identifying internal audit's role in the project. Phase 2 priorities should include improving system performance and test processes to reduce spurious output. Assessing available data and performing various types of testing of data sets are crucial in phase 3. In phase 4, the KRIs should be identified by addressing trending information on usage and service quality, completeness and

accuracy of data, and disaster recovery capabilities. Finally, the focus in phase 5 should be on speed, indexing, and assessing storage and cloud options (private versus internal storage or public versus hybrid cloud) to create efficiencies.

The five phases often overlap and might not occur in sequence. In addition, both risk management professionals and senior management have specific tasks they must accomplish during each phase to make the plan work.

The bottom line: Auditors, risk managers, and compliance officers must work with senior management to understand and embrace big data to help identify and mitigate risks. Plus, they should take advantage of the opportunities big data offers to improve their own effectiveness. By covering risks and opportunities, they can help organizations analyze and understand big data's potential from both a compliance perspective and a strategic and operational improvement stance. [la](#)

ROB BLANCHARD, CISA, is a senior manager with Crowe Horwath LLP in Columbus, Ohio.

KEVIN O'SULLIVAN, CISA, is a principal with Crowe Horwath LLP in New York.



Engage and Connect Globally

Gain a competitive edge with unique IIA advertising and sponsorship opportunities as diverse as the 180,000 members in the 190 countries we serve.

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

www.theiia.org/goto/advertise



2015-1635

From Classrooms to Boardrooms: Academic Relations Helps Prepare Students for a Career in Internal Auditing



The IIA offers two programs to help fill the pipeline with “internal audit-ready” graduates to enter the business arena: The Internal Audit Academic Awareness Program and the Internal Auditing Education Partnership (IAEP).

Our efforts are made possible through the Internal Auditing Academic Advancement Fund (IAAAF). Since 2006, the IAAAF awarded more than \$1.3 million in grants to universities around the globe to fund teaching assistants, curriculum development, and scholarships for IAEP students.

Help us continue to develop internal audit-ready students and provide them with a rewarding career path.

Support The Internal Auditing
Academic Advancement Fund today!

www.theiia.org/Academic





BY J. MICHAEL JACKA

40 HOURS OR FOREVER

Audit training should go far beyond just logging a requisite number of hours.

For as many years as I can remember, our audit department's annual budget included 40 hours of training for each auditor. Some auditors used their time; most did not. But year after year we doggedly entered our optimistic estimate that each auditor would invest those 40 hours. Apparently, we weren't the only ones.

Larry Harrington, IIA global chairman of the board, has adopted the theme, "Invest in Yourself" for his chairmanship. Let's start by admitting it is a bit sad that we have to be reminded that a personal investment in learning is important. Nonetheless, research shows that the 40-hour allotment is true for most audit departments—and it has been true for a long time.

Harrington emphasizes that an increase in training time is necessary and that auditors must broaden their knowledge of internal audit and the business. And because studies indicate that some of our clients are questioning internal audit's knowledge and business acumen, it is hard to argue with this recommendation.

Still, I don't think it goes far enough.

Whether investing 40 hours, 50 hours, or more, only the bare minimum can be achieved when training merely involves clocking hours. I have seen far too many auditors sitting in meetings, conferences, luncheons, and other events taking notes that will never be read, listening to words that will not be heeded, and putting in the minimum requirement of attention necessary to gain precious continuing professional education credits. In fact, I've seen these people sitting in some of my own presentations. The words flow around them, they clock the hours, and they say they've been "trained."

The problem is that we focus on training. What we need is real learning.

Real learning is not about 40 hours. It is about an unconstrained thirst for knowledge. It is about succumbing to inquisitiveness. It is about passion for a subject that is not restricted to the classroom, office, or convention hall. Real learning is about spending forever in the pursuit of knowledge because there is just so much to know.

And effective learning should not be pigeonholed. New ideas can spring from anywhere. History is rife with examples of unconnected concepts coming together to make great leaps. So, while pursuing knowledge about internal audit and the business, auditors should also recognize that effective learning can happen in any discipline.

Harrington shares another important concept—the need for internal auditors to be agents of transformation. We need new ideas, we need new thoughts, and we need new knowledge. If we stay the way we are, we will become forgotten relics of the past. As agents of transformation—transforming the profession and transforming business—we will be part of an important future. But to do that, we must remain inquisitive and never be satisfied with how much we know, let alone being satisfied with 40 hours of training. [la](#)

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

GRC IN TODAY'S BUSINESS ENVIRONMENT

Organizations need to take a balanced, integrated approach to achieving objectives, managing risks, and complying with regulations.



NOAH GOTTESMAN
Director of Audit
Advisory & Innovation
Thomson Reuters



SERGIU CERNAOTAN
Director, GRC Strategy
ACL

How do you define GRC?

CERNAOTAN There are a lot of GRC definitions out there, and they can be overwhelming to sort through. My company likes to think of it in the broadest possible terms and has found the Open Compliance and Ethics Group definition to be the most encompassing. Essentially, governance is preoccupied with achieving organizational objectives. Risk management is focused on managing the uncertainty of achieving organizational objectives. And, compliance is the mechanism to ensure companies act with integrity while in pursuit of their objectives. **GOTTESMAN** It is a broad concept that aligns the top-down and bottom-up perspectives of the organization across geographies and various management bifurcations. I normally equate it to “balance” — we all strive to achieve it, but it is truly never perfect.

What comprises an effective GRC strategy?

GOTTESMAN An effective GRC strategy includes the active involvement of an organization's directors, executives, and frontline personnel in coordinating and collaborating with the many layers of services provided by management, risk and compliance, and audit. At the core of the GRC strategy is the unifying mandate on how the organization comes together to achieve objectives, manage and mitigate risks, and comply with regulations, standards, and frameworks. **CERNAOTAN** Most GRC strategies focus on the defensive posture of mitigating risk. That is good, but many stop there. An effective GRC strategy involves not just risk mitigation, but it also should help organizations take appropriate, profitable risks, essentially helping them maximize the risk-reward ratio. Sometimes, the biggest risk is not taking a risk at all.

What are the biggest compliance risks your clients are talking about?

CERNAOTAN With an ever growing list of requirements, many clients are concerned with the risk of completeness—the fear that they have failed to consider a significant compliance risk. A second concern is whether they have an adequate mechanism to provide a timely and accurate warning of the risk or degree of noncompliance with known requirements. **GOTTESMAN** The biggest compliance risk continues to be around internal controls, whether it is dealing with the U.S. Dodd-Frank Act of 2010, the Foreign Corrupt Practices Act, adherence with The Committee of Sponsoring Organizations of the Treadway Commission's updated *Internal Control—Integrated Framework*, or finding a middle ground with the external auditors who are under increased pressure from the Public Company

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



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

Accounting Oversight Board, especially after the Board's Staff Audit Practice Alert 11, Considerations for Audits of Internal Controls Over Financial Reporting. The documentation, testing, and monitoring of internal controls requires more governance from both the top and the bottom of the organization.

How can the various compliance, risk, control, and assurance functions better align?

GOTTESMAN These functions can better align by sharing their perspective of the organization and the core components of their methodology; specifically: how they view the organization, how they assess it, how they prioritize activities, how they execute on those activities, how they document results, how they determine the significance and priority of their results, and how they plan to follow up on their results.

CERNAUTAN The design of traditional GRC functions prevents them from being conducive to alignment from the start. GRC responsibilities are usually viewed as bolt-on activities and delegated to certain departments or individuals, such as internal audit or the chief risk officer. As such, they are viewed as "someone else's job" by management and as "interfering

with doing my real job" by the business. Better alignment is achieved when the responsibility for GRC is integrated into the day-to-day duties of process owners from every role and function in proportion to their impact on the business.

How are your compliance clients addressing regulatory fatigue and increased liability for compliance failures?

CERNAUTAN Customers are realizing that having an integrated GRC system to administer regulatory compliance programs is critical to handling the burden of regulatory fatigue, similar to having an ERP system for handling accounting and operational complexities. Also, customers are recognizing the importance of having a regulatory content management solution that is integrated with their GRC platforms to stay abreast of changing and emerging regulations.

GOTTESMAN Clients are turning a very reactive, conservative posture into a more proactive position. Globally, regulations are changing and evolving; it is no longer just about the compliance outcomes and much more about day-to-day decisions made beforehand. It requires compliance and internal audit departments to share their approaches to regulations. [la](#)



Responsive. Intuitive. Enhanced. The *Internal Auditor* Website Delivers More

Garner internal audit insight like never before with access to the current/archived content, exclusive online features, blogs, and video with optimized options to search and comment/share.

Go experience InternalAuditor.org.

Ia
INTERNAL AUDITOR

2015-1636



BY GUILLAUME LITVAK

A COMMITMENT TO CHANGE

To dispel negative perceptions, internal auditors must keep a sharp focus on delivering stakeholder value.

Internal audit's image, though considerably better than it was years ago, still needs some improvement in the eyes of those we serve. According to recent surveys, stakeholders often see the profession as disconnected from business priorities and mired in outdated practices. Audit functions that maintain such practices and refuse to move forward do a disservice to the organization and damage the profession's reputation. To change negative perceptions and provide the level of service our organizations require, we need to adjust our mind-set, sharpen our communications, and actively seek to gain the trust and respect of stakeholders.

Changing our mind-set means adopting a focus on working with the business toward the shared purpose of improvement. Auditors more often than not are expected to identify deficiencies and offer critiques, making them seem rigid and adversarial. Adjusting this perception is essential—and it can be done in surprisingly simple ways. For instance, auditors could dedicate 25 percent of their time on each engagement to identifying best

practices, and then share those practices across the organization. They could also supplement their traditional assurance mission by allowing another 25 percent of their time for advisory work. In addition to benefiting the client, this approach can help change how internal audit is perceived and increase the likelihood that the function's support will be requested in the future.

This shift in audit focus will not succeed, however, without a way to ensure our message reaches the client. Realistically, how much time does top management dedicate to reading the final audit report? Perhaps somewhere between 30 seconds and two minutes? We need to create our reports with our clients' busy schedules and competing demands in mind. We must prioritize information to include in the report, convey that information succinctly, and enhance content presentation with effective use of visuals. There's no point to working hard for several weeks, interviewing dozens of people, and analyzing hundreds of documents, only to produce an audit report that no one reads.

Finally, to gain stakeholders' attention and trust, we must demonstrate a strong commitment—and even passion—for our work. Are you truly passionate about your organization's products and innovation? Are you spending some time every day reading news about your industry, staying abreast of relevant technology, and meeting with your colleagues to understand their priorities and concerns? We need to show enthusiasm for the businesses we serve and think regularly about how we can contribute to the organization's success.

When each of these factors is in place, the audit team will be seen as an invaluable asset and committed to organizational improvement. Demonstrating that internal audit is focused on making a contribution to the business and genuinely interested in its success will help dispel audit stereotypes and earn management's trust. We can then move beyond the negative perceptions and concentrate on delivering the value our clients deserve. [\[a\]](#)

GUILLAUME LITVAK is CAE at Technicolor in Paris.

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

The Framework for Internal Audit Effectiveness: The New IPPF

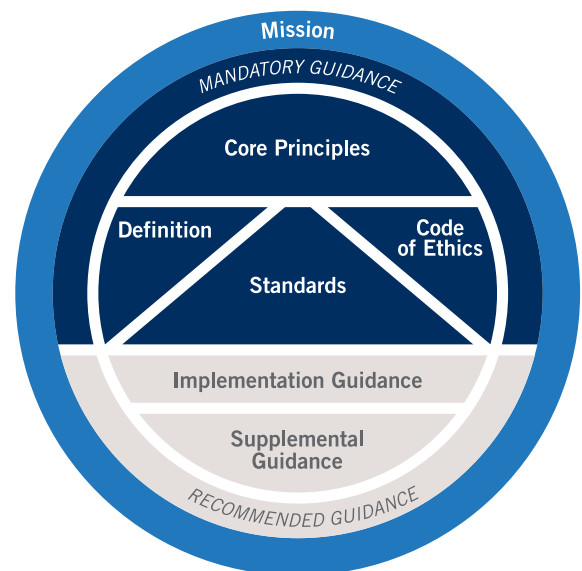


International Professional
Practices Framework

Changes in today's business environment and the associated risks are only accelerating.

Internal auditing requires commitment and a framework of clearly articulated principles, leading-practice standards, and timely guidance that not only acknowledges but also anticipates these changes.

For internal audit to keep up with an ever-changing environment, the International Professional Practices Framework® (IPPF®) must evolve to effectively support the profession and meet the many challenges ahead — a changing risk landscape, growing stakeholder expectations, and increasing legislative and regulatory demands for improved governance, risk management, and internal control.



Learn more about the new IPPF, download the new implementation guidance, and understand the enhancements that lie ahead. www.theiia.org/goto/IPPF

CBOK Updates for Financial Services Auditors

The Institute of Internal Auditors' 2015 Global Internal Audit Common Body of Knowledge (CBOK) Practitioner Survey offers insights into the outlook for financial services organizations. This survey report takes a closer look at the top six challenges for internal auditors:

- Addressing regulatory compliance risks
- Adapting to crowded governance committee agendas
- Contending with heightened expectations
- Responding to increasing technology risks
- Integrating recommended lines of defense
- Managing resource allocations

To get the details on these trends, including summary results from the study, visit www.crowehorwath.com/CBOK or contact Jennifer Burke at +1 859 280 5160 or jennifer.burke@crowehorwath.com.

Jennifer Burke
Partner, Crowe Horwath

