Ia
INTERNAL AUDITOR

OCTOBER 2016

INTERNALAUDITOR.ORG

COSO Framework at the Heart of Boeing Internal Audit

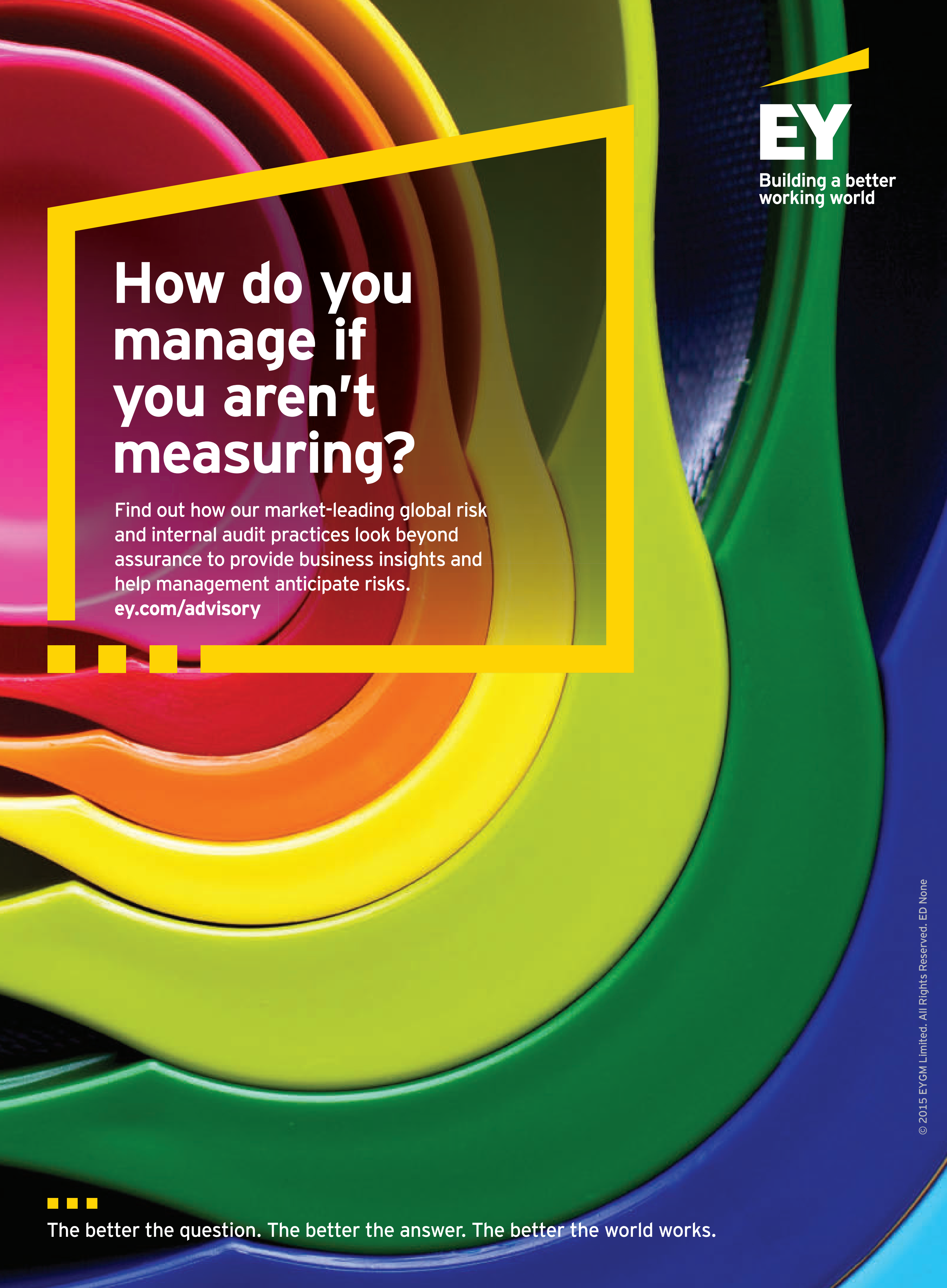
Balancing Employer/Employee Privacy Needs

A Coordinated Approach to Compliance and Internal Audit

The Power of Rhetoric

NONFINANCIAL REPORTING

Internal audit is best positioned to provide assurance and insight on the overall health of the organization.



ARE YOU PART
OF THE 57%*?
*% of companies where Internal Audit is performing well at leveraging analytics and technology

Source: PwC State of the Internal Audit Study, 2014-2016

BE PART OF THE GROWING TREND

IDEA 10® makes it easy to analyze 100% of your data, visualize patterns and discover anomalies so you can share timely insights with your organization.

Learn how to get started with a data analytics program.
Visit casewareanalytics.com/57trend

CASEWARE ANALYTICS

IDEA is a registered trademark of CaseWare International Inc.

Ia
INTERNAL AUDITOR

CELEBRATING 75 YEARS OF THE IIA

OCTOBER 2016 VOLUME LXXIII: V

FEATURES

Working in Concert to
Help You Perform

Ia
INTERNAL AUDITOR

CELEBRATING 75 YEARS OF THE IIA

OCTOBER 2016 VOLUME LXXIII: V

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org

Bashing the Boss Online Even outside of the workplace, employees need to be mindful of what they say about the organization on social media sites – and internal auditors need to understand the potential impact.

Worldwide Risk and Opportunity Watch former Australian Prime Minister Julia Gillard discuss geopolitical risk, the rise of Asia, and challenges for multinational organizations.

Building on a Foundation of Fraud Art Stewart looks at the risks of programs meant to aid minority- and women-owned businesses.

Reporting on Cyber Threats Internal audit should reevaluate its criteria for reporting IT issues to the audit committee and senior executives.

Find us on Facebook

Internal Auditor ISSN 0020-5745 is published in February, April, June, August, October, and December. Yearly subscription rates: $75 in the United States and Canada, and $99 outside North America. No refunds on cancellations. Editorial and advertising office: 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. Copyright © 2016 The Institute of Internal Auditors Inc. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Altamonte Springs, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 247 Maitland Ave., Altamonte Springs, FL 32701-4201, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001. Opinions expressed in *Internal Auditor* may differ from policies and official statements of The Institute of Internal Auditors and its committees and from opinions endorsed by authors' employers or the editor of this journal. *Internal Auditor* does not attest to the originality of authors' content.

COVER: PHOTO ILLUSTRATION BY SEAN YATES,
TOP: JIRSAK / SHUTTERSTOCK.COM, BOTTOM: OLLYY / SHUTTERSTOCK.COM

Crowe Horwath.

Cybersecurity resilience – go beyond security to a new level of readiness.

Access our latest article outlining the critical components your organization needs for a mature and effective cyber program.

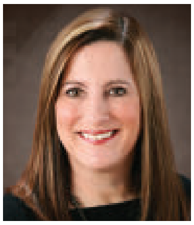
crowehorwath.com/cyberresilience

Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

In accordance with applicable professional standards, some firm services may not be available to attest clients.

RISK-17010-015C



WHAT'S IN A NAME?

Nonfinancial reporting, integrated reporting, holistic reporting, or enhanced reporting—although there's no single, agreed-upon name for this type of reporting (even among the editors of this magazine), stakeholders and investors agree on the need for more comprehensive reporting that goes beyond the financial health of the organization.

According to The IIA Global Perspectives and Insights report, Beyond the Numbers: Internal Audit's Role in Nonfinancial Reporting, this type of reporting "fills the void by reporting quantitative and qualitative information that falls outside the scope of mainstream financial statements." In this month's cover story, "Taking the Lead on Nonfinancial Reporting," author Arthur Piper considers the disclosure of nonfinancial information and the leading role internal audit can play because of its knowledge of the organization.

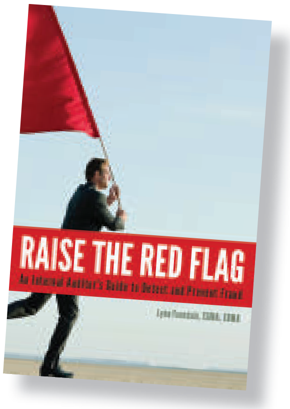
The nonfinancial reporting movement appears to be slightly further along in Europe than in other parts of the world. By December, governments across Europe will need to have translated the European Union's 2014 Directive on nonfinancial reporting into their national rule books. The directive requires organizations to disclose information on environmental issues, social and employee-related matters, respect for human rights, and anti-corruption and bribery. And although the terminology may not yet have caught on in the U.S., Jim Pelletier, The IIA's vice president of Professional Solutions, points out in the cover story that internal auditors who are taking a risk-based approach and are looking at the major objectives of the organization are likely to be addressing nonfinancial areas.

Continuing with the reporting theme, but in another vein, I'm excited to report *Internal Auditor* has a new "Fraud Findings" contributing editor. Bryant Richards, a member of The IIA's Publications Advisory Committee and the magazine's Editorial Advisory Board, is an associate professor of accounting and finance at Nichols College in Dudley, Mass. Previously, he was the director of corporate governance for the Mohegan Tribal Gaming Authority. Welcome, Bryant!

Anne

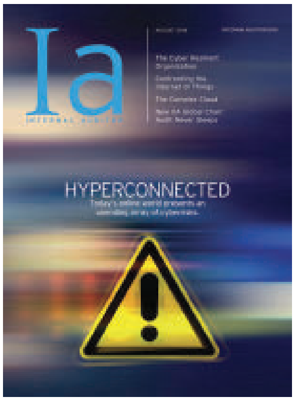
@AMillage on Twitter

Help Your Organization
Identify the Risk of Fraud
Before It's Too Late


RAISE THE RED FLAG
An Internal Auditor's Guide to Detect and Prevent Fraud
Lynn Fountain, CGMA, CRMA

Reader Forum

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



Data Fever

Mike Jacka has correctly diagnosed the disease affecting many who are hot for data analytics. "Ready, aim, fire" is still the best approach. You need to know what you want to achieve before you start developing analytics. So many feverishly rush to use the shiny new tools, when what we should be doing first is asking: a) What are the risks that matter most to the organization and its achievement of objectives? and b) How can we assess the management of those risks? Analytics can be great, but only if they are used when we are ready and can aim them at the risks that matter.

NORMAN MARKS *comments on Mike Jacka's "Do You Have Data Fever?" ("Mind of Jacka," August 2016).*

I agree with Mike Jacka when he says, "auditors should talk with the data owners to understand what is available, how it is used, and how it relates to the processes under review." Sometimes this becomes a challenge because the data owners talk about how helpful and value-added their processes are without actually answering your questions. Therefore, receiving a data dump can be useful in performing basic tests first (e.g., testing for missing fields, duplicates where unique values should be, and double payments and receipts). Then more specific testing also can be performed after a walkthrough is received from the data owner for one entire data sample that outlines key controls, or lack thereof.

OWAIS RIZVI *comments on Mike Jacka's "Do You Have Data Fever?"*

The CAE Challenge

We have a saying in Arabic that goes something like, "The notch is bigger than the patch." The CAE is faced with a real challenge and will continue to be as long as he or she serves multiple interests. His or her boss, the audit committee, and investors-at-large naturally have conflicting interests with the pressure of targets, competition, and so on.

ABDULKAREEM ALYOUSIF *comments on the Chambers on the Profession blog post, "When Internal Audit Finds Itself at the Plaintiff's Table."*

Conflicts of Interest

It is very important to have a policy for conflicts of interest. Additionally, a single person should not be given authority to carry out a transaction from start to finish. Segregation of duty, dual signatory, and conflict of interest policies also are important controls that need to be enforced at the entity level. Internal audit should use data analytics to understand transactions that are normal and transactions that seem abnormal.

MANOJ AGARWAL *comments on James Bailey's "Fraud and Related-party Transactions" (June 2016).*

Culture and Communication

I agree that the governance, risk, and controls culture is a necessity in any company. But the implementation of

Ia
INTERNAL AUDITOR
OCTOBER 2016
VOLUME LXXIII: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
J. Michael Jacka, CIA, CPCU, CFE, CPA
Steve Mar, CFSA, CISA
Bryant Richards, CIA, CRMA
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
David Coderre, CPM
Michael Cox, FIIA(NZ), AT
Dominic Daher, JD, LLM
Haley Deniston, CPA
Kayla Flanders, CIA, CRMA
James Fox, CIA, CFE
Peter Francis, CIA
Michael Garvey, CIA
Nancy Haig, CIA, CFE, CCSA, CRMA
Daniel Helming, CIA, CPA
J. Michael Jacka, CIA, CPCU, CFE, CPA
Sandra Kasahara, CIA, CPA
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
Bryant Richards, CIA, CRMA
Jeffrey Ridley, CIA, FCIS, FIIA
Marshall Romney, PHD, CPA, CFE
James Roth, PHD, CIA, CCSA
Katherine Shamai, CIA, CA, CFE, CRMA
Debora Shelton, CIA, CRMA
Laura Soileau, CIA, CRMA
Jerry Strawser, PHD, CPA
Glenn Sumners, PHD, CIA, CPA, CRMA
Sonia Thomas, CRMA
Stephen Tiley, CIA
Robert Venczel, CIA, CRMA, CISA
Curtis Verschoor, CIA, CPA, CFE
David Weiss, CIA
Scott White, CIA, CFSA, CRMA
Benito Ybarra, CIA

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

IIA CHAIRMAN OF THE BOARD
Angela Witzany, CIA, QIAL, CRMA

PUBLISHED BY THE
INSTITUTE OF INTERNAL
AUDITORS INC.

CONTACT INFORMATION

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

SUBSCRIPTIONS, CHANGE OF ADDRESS, MISSING ISSUES
customerrelations@theiia.org
+1-407-937-1111; fax +1-407-937-1101

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

PERMISSIONS AND REPRINTS
editor@theiia.org
+1-407-937-1232; fax +1-407-937-1101

WRITER'S GUIDELINES
InternalAuditor.org (click on "Writer's Guidelines")

Mobile
Webinars
Online
Specialty Audit Centers
Ia
Print
Foundation Partnerships
Conferences

this culture will call for an important effort of communication, and for a good dose of personal will from the board of directors.

PRISCILLE KONA *comments on the Chambers on the Profession blog post, "If Strategy Is Culture's Breakfast, Then Governance, Risk, and Controls Are Its Appetizers."*

Limiting Ourselves

As internal audit teams, we should be able to answer the question, "Why am I here?" or rather, "What should my organization be getting from internal audit?" Most people's resumes (including auditors) will tell you they want "to make a difference" in their job. Jacka points out that we just give customers what they think they want, instead of "what we know we can deliver." I think we should not just limit ourselves to what we know we can deliver, but actually push ourselves to deliver what our organization needs and deserves. If that means we need to bring in outside specialist skills, or increase skills in-house, then we should do that.

I love the old joke: Why did the auditor cross the road? Because that's what they did in the prior year working paper! It brings me to the audit-business-impact-dilemma: How can someone who can't innovate for themselves advise others regarding innovation and opportunity identification?

ANNARIE OOSTHUIZEN *comments on the From the Mind of Jacka blog post, "Does Internal Audit Kill Organizational Innovation?"*

Whistleblower Protection

CAEs need whistleblower protection, too. I also think CAEs should be incentivized, under federal law, for reporting truthful information regarding unethical and/or illegal behavior at both the state and federal levels. The IIA should follow Richard Chambers and unite our collective voice ensuring fair treatment for Richard Patton. The investigation into Patton should be fully disclosed to taxpayers. Let the facts speak.

ZACH ZEMENICK *comments on the Chambers on the Profession blog post, "Is Houston Another Place Where Oversight Goes to Die?"*

MORE **VISIT InternalAuditor.org for the latest blogs.**

Regulation hampers AML efforts... Study ranks national cybersecurity... Governance expectations changing... Intercompany accounting problems.

Update

GREAT CULTURE, GREAT CEO

Employees favor CEOs when they are satisfied with their company's culture.

Corporate culture is the strongest factor in employee ratings of their organizations' CEOs, according to What Makes a Great CEO?, a report by Mill Valley, Calif.-based employment and recruiting website Glassdoor. In fact, a one-level increase in overall company ratings on a five-star scale—from three stars to four stars, for example—raises CEO approval ratings in large, publicly listed companies by nearly 37 percent, the report notes. "In the eyes of many employees, CEOs are ultimately held accountable for workplace culture," the report observes.

The Glassdoor findings are based on 1.2 million CEO approval ratings for about 70,000 U.S. employers that were collected in its company review survey. Researchers then looked at factors that might influence CEO approval ratings, using data from external sources on CEO pay, tenure, and company profitability.

Opinion of senior leadership, view of career opportunities, and quality of compensation and benefits are the cultural factors that have the greatest impact on CEO approval ratings. Among cultural factors, work-life balance is the exception, surprisingly—CEO approval is lower in organizations with high work-life balance.

Aside from company culture, CEOs of more profitable companies receive the

ENFORCEMENT ACTIVITY DIPS

The U.S. Securities and Exchange Commission has brought fewer enforcement actions so far in fiscal year 2016.

2015 actions Q1-3

555

2016 actions Q1-3

508

Source: Cornerstone Research, analysis of enforcement actions Identified at www.sec.gov

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

IMAGES: TOP, JIRSAK / SHUTTERSTOCK.COM, RIGHT, JOHN T. TAKAI / SHUTTERSTOCK.COM

highest approval ratings. Moreover, CEOs who are company founders have higher approval ratings than executives who were promoted internally or hired externally. The highest-rated CEOs are in the real estate, construction, IT, and finance industries, while the lowest rated are in the retail, manufacturing, transportation, and mining sectors.

CEO pay has the greatest negative impact on CEO approval, with the highest-paid CEOs receiving the lowest approval ratings and the lowest paid receiving the highest approval ratings. Even here, the data suggest that "the negative effect of higher CEO pay on CEO approval ratings can be partly ameliorated if it is accompanied by great company culture." **— T. MCCOLLUM**

19%

OF CONSUMERS WOULD STOP SHOPPING AT A RETAILER THAT HAS HAD A CYBERSECURITY BREACH

55%

OF SENIOR IT EXECUTIVES AT RETAILERS HAVE NOT INVESTED IN CYBERSECURITY WITHIN THE PAST 12 MONTHS

"Consumers are clearly demanding that their information be protected, and they're going to let their wallets do the talking," says Mark Larson, KPMG's national line of business leader for Consumer Markets.

Source: KPMG, 2016 Consumer Loss Barometer Report

ILL-EQUIPPED FOR ANTI-MONEY LAUNDERING

Regulatory complexity has executives worried about inadequate staff and resources.

Seventy-nine percent of 280 senior-level executives of financial institutions surveyed are moderately or very concerned about enterprisewide compliance and the integration of their anti-money laundering (AML) programs, according to a recent survey from financial services technology provider NextAngles. Challenges cited around AML programs include the introduction of new regulations (77 percent) and staffing concerns (76 percent).

"The survey shows increasing anxiety among financial institution executives that they are insufficiently staffed and equipped for today's compliance challenges," NextAngles CEO Mallinath Sengupta says.

Respondents say their AML programs are challenged by staffing issues such as the competitive job market, shortage of qualified applicants, and restricted budgets.

Nearly two-thirds of respondents expect their AML compliance spending to increase by at least 5 percent within the next 18 months. Similar findings in Financial Crimes Survey 2016, from *Operational Risk* magazine and BAE Systems, indicate that 51 percent of the 204 respondents expect budgets to rise in the next three years. **— S. STEFFEE**

STUDY RANKS CYBER AWARE COUNTRIES

Fourteen countries are recognized for promoting cybersecurity preparedness.

The U.S. ranks No. 1 among the most cyber aware countries, according to a recent study by cybersecurity distributor Turrem Data. The rankings are based on the Global Cybersecurity Index issued by ABI Research and the International Telecommunication Union. In addition to the ranking, the study discusses what countries can do to prepare for potential cyberattacks and implement protection plans.

The compiled data identifies five indicators of cybersecurity preparedness that governments should look

IMAGES: TOP, SPECTRAL-DESIGN / SHUTTERSTOCK.COM, RIGHT, AFRICA STUDIO / SHUTTERSTOCK.COM

VISIT InternalAuditor.org to view a video interview with Julia Gillard.

at to improve their nation's cyber awareness: legal measures, technical measures, organizational measures, capacity building, and cooperation. The study recognizes the U.S. for best practices such as its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Critical Infrastructure Protection Program.

Canada ranks second because it requires federal agencies to have an IT security strategy and has seven institutions that promote cybersecurity. Australia, Malaysia, and Oman are tied for third for having computer crime and consumer protection operations, relations with other national CERT agencies, and cybersecurity strategies and plans. Rounding out the rankings are New Zealand, Norway, Brazil, Estonia, Germany, India, Japan, South Korea, and the U.K.

The study notes that three countries—China, Russia, and Switzerland—did not make the list because of their lack of progress in building cybersecurity capacity. Switzerland, especially, was expected to be ranked because it is home to several important international organization headquarters such as the European Organisation for Nuclear Research and the World Economic Forum. Such lack of cybersecurity preparedness is common in most countries, though, the report says.

– NICOLE LICOURT

TRANSPARENCY OFFERS REASSURANCE

Expectations about what good governance is changes over time, says former Australian Prime Minister **JULIA GILLARD**.

How important is good corporate governance to a strong national economy? Good corporate governance is vital to a strong national economy. Unless people can transparently see what is happening in an economy, they can't properly calibrate risks and opportunities. So around the world we see patterns of investment going into economies that have good governance and transparency and can offer people reassurance. That's something that, as prime minister in Australia, we were always very proud of. But it's something you've got to keep building because norms and expectations about what good governance is changes over time.

Given Australia's ties with Great Britain, how will the Brexit vote impact Australia's trade? For Australia, the real implication of the Brexit vote is not so much a trade implication. Our trade relationships are very diversified, and much of our trade is in our own region of the world, particularly with China, and with the U.S. The thing that is most flowing through Australian political discourse about Brexit is the sign it sends that around the world there is a lot of disgruntlement with the impact of globalization – a lot of turning away from internationalism – and, ultimately, that could affect every nation on earth as people seem to be losing faith in global structures.

INTERCOMPANY ACCOUNTING FALLS SHORT

A recent poll finds coordination lacking among organizational legal entities.

More than two-thirds of the 3,800 finance and accounting professionals polled by Deloitte say their organizations are working toward greater consistency in intercompany accounting, but they haven't yet achieved it. Less than 10 percent indicate their organization has a holistic accounting framework with efficient systems and communications across critical functions.

Deloitte defines *intercompany accounting* as "processing and accounting for internal financial activities and events that impact multiple legal entities within a company." It can include sales of products and services, fee sharing, cost allocations, royalties, and financing activities.

Intercompany accounting "can become a real challenge to those experiencing global growth, mergers and acquisitions, and supply chain integration," says Kyle Cheney, a Deloitte Advisory partner. Disparate software systems are respondents' greatest intercompany accounting issue. **– D. SALIERNO**

IMAGES: RIGHT, ALPHASPIRIT / SHUTTERSTOCK.COM

Back to Basics

BY ANUPAM GORADIA EDITED BY JAMES ROTH + LAURA SOILEAU

THE ART OF RECOMMENDING

Internal auditors walk a fine line when presenting recommendations to management.

One of the ways internal audit adds value to the organization is through the recommendations communicated in internal audit reports. But recommendations also can become a point of contention with management, as they may suggest additional procedures for staff or offend management if not presented correctly. Therefore, auditors should take care to communicate with the various stakeholders how their recommendations will help fix gaps and mitigate risks. The stakeholders will evaluate whether the recommendations being provided are worth the investment of time and resources required to implement them (cost vs. benefit).

Recommendation Types

Broadly, a recommendation is either a suggestion to fix an unacceptable scenario or a suggestion for improvement. Most internal audit reports provide recommendations to fix unacceptable scenarios because they are easy to identify and are less likely to be disputed by the process owner. However, recommendations to fix gaps in a process only take the process to where it is expected to be and not where it *could* be. Internal audit's value lies not only in providing solutions to existing issues but in instigating thought-provoking discussions. Recommendations also can include suggestions that will move the process or the department being audited to the next level of efficiency. When recommendations aimed at future improvements are included, internal audit reports become a tool in shaping the strategic direction of the department being audited.

Internal and External Sources

An auditor should draw recommendations from both inside and outside the organization (see "Sources of Recommendations" on page 19). Internal sources of recommendations are easier to locate; however, they require a tactful approach as process owners may not be inclined to share unbiased opinions with internal audit. External sources may not be as easily accessible—an internal audit function should invest in providing its staff with access to research libraries and professional networks to facilitate access.

It is a good practice to jot down recommendation ideas as soon as they come to mind, even though they may not find a place in the final report. Even if internal audit testing does not result in a finding, the auditor may still recommend improvements to the current process.

Documentation

Internal audit should spend sufficient time brainstorming potential recommendations

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

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

and choosing their wording carefully to ensure their audience has complete understanding. Recommendations should be written simply and should:

- Address the root cause if a control deficiency is the basis of the recommendation.
- Address the department rather than a specific person.
- Include bullets or numbering if describing a process that has several steps.
- Include more than one way of resolving an issue identified in the observation, if possible. For example, sometimes a short-term manual control is suggested as an immediate fix in addition to a recommended automated control that will involve considerable time to develop.
- Position the most important observation or risk first and the rest in descending order of risk.
- Indicate a suggested priority of implementation based on the risk and the ease of implementation.
- Indicate any repeat findings. If the recommendation needs to be modified, provide an updated recommendation in the report.
- Explain how the recommendation will mitigate the risk in question.
- List any recommendations separately that do not link directly to an audit finding but seek to improve processes, policies, or systems.

Management Feedback

Recommendations will go nowhere if they are not valued by management. Therefore, the process of obtaining management feedback on recommendations is critical to make them practical. Ultimately, process owners may agree with the recommendation, agree with part of the recommendation, and agree in principle, but technological or personnel resource constraints won't allow them to implement it. They also may choose to revisit the recommendation at a future date as the risk is not imminent, or disagree with the recommendation because of varying perceptions of risk or mitigating controls.

Management in the public sector could be averse to recommendations because of public exposure of their reports. Therefore, internal audit should clearly state in its reports if the recommendations do not correspond to any errors but are suggested improvements. More recommendations do not mean there were more faults with the process, and this should be communicated to the process owners.

Management responses should be added to the recommendations with identified action items and implementation timelines whenever possible. Whatever management's response, a recommendation should not be changed if it dilutes internal audit's objectivity and independence and becomes representative of management's opinions and concerns. It is internal audit's prerogative to provide recommendations, regardless of whether management agrees with them. Persuasive and open-minded discussions with process owners are important to achieving agreeable and implementable recommendations.

SOURCES OF RECOMMENDATIONS

Internal

- Process owner walkthroughs.
- Critical reading of documented procedures.
- Practices followed by other departments or locations within the organization.
- Prior internal audit reports on the area currently being audited.
- Results of current testing.
- Recommendations in other internal audit projects.

External

- IIA research materials.
- Other professional and industry literature.
- Networking with industry peers.
- Procedures followed by other organizations.
- Vendor-provided education on new technologies and services related to the process being audited.

A Complex Journey

The journey of a potential suggestion to a recommendation is complex and is influenced by every stakeholder and constraint in the audit process—be it the overall tone of the organization toward change, its philosophy toward internal audit, the scope of the internal audit, views of the process owner, experience and exposure of internal audit staff, or available technology. However, an internal auditor must realize that every thought may add value to the organization and deserves consideration within the internal audit team. Internal audit departments should deliberate about the process and ask at the end of every audit: Does it align with the organization's strategy and direction? Is it up to par with what is seen elsewhere? What is its relevance today and in the future? Ia

ANUPAM GORADIA, CPA, CISA, CITP, *is a senior manager in the Risk Advisory division at WithumSmith+Brown CPAs and Consultants, New Brunswick, N.J.*

BY LORRAINE LEE EDITED BY STEVE MAR

BIG DATA AND INTERNAL AUDITORS

Today's data analytics expand auditors' ability to tap into all types of information generated by the organization.

Big data has greatly expanded the amount of information available to internal auditors. Organizations now store an enormous amount and variety of data, ranging from traditional financial data associated with sales and expenses to more unstructured data associated with video, weblogs, email, and tweets.

Data-savvy internal audit groups are mining this data to generate actionable insights and recommendations. For example, the ability to analyze large data sets can enable internal auditors to examine all cash expenses, not just a sample, and determine whether any employees are consistently submitting an inappropriately high volume of cash expenses. Another example would be reviewing the types and amounts of purchase card transactions made by all departments for anomalies.

Data analytics makes it possible for auditors to discover and report on meaningful patterns and insights derived from large and complex data sets through the use of statistics and other types of quantitative analysis. Audit analytic tools and data visualization software, coupled with the massive data storage capacity of data centers, have created an opportunity for internal auditors to exploit an organization's data to improve the internal audit function's performance.

The Four V's of Big Data

Big data has four specific attributes: volume, variety, velocity, and veracity. *Volume* refers to the amount of data available. According to IBM, the world is generating 2.5 exabytes (2.5 billion gigabytes) of data daily. The most obvious impact this vast amount of data has on the internal audit function is the capacity to greatly improve audit coverage. Instead of selecting a limited sample of transactions to test, an auditor now can analyze all of the transactions in an audit population.

Variety refers to the various types of data being generated, both structured and unstructured. Ninety percent of data is unstructured, including text, photos, audios, videos, click streams, and log files. Access to such a variety of business documents can enable auditors to analyze larger, nontraditional data sets and perform more detailed analysis.

Velocity refers to the increasing speed in which the data is created, as well as the speed in which it can be processed, stored, and analyzed. Greater velocity enables continuous auditing of audit evidence on a frequent, repeatable, and sustainable basis. Although the concept of continuous auditing has been around for more than 20 years, the software and hardware associated with big data is making continuous auditing a reality for internal audit groups.

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

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

Finally, *veracity* refers to the quality and trustworthiness of the data to be relied on to draw accurate conclusions. The volume, variety, and velocity of data is only useful if that data is correct, consistent, and complete. IT audit processes such as those associated with assurance in areas such as backup and restore, disaster recovery planning, data storage, data security, and access control are critical in ensuring the veracity of the organization's data.

Visualizing Data

In addition to the Four V's, internal auditors should consider a fifth aspect of big data: visualization. Data visualizations are presentations of data in a pictorial or graphical format that enables decision-makers and auditors to view a visual representation of the data. An effective visualization facilitates the understanding of difficult concepts or identifies new patterns or trends from the data.

> **Data trends can provide insights into the risks facing an organization.**

Recent advances in user-friendly data visualization software are enabling auditors to easily extract and analyze data and create visualizations and storyboards from that data. This helps auditors find and communicate meaning from the data. In addition, visualization tools support the detailed analysis of large, nontraditional data sets and provide the means for internal auditors to more effectively communicate insights from their organization's data.

Adding Analytics to Audits

To incorporate data analytics in their internal audit operations, auditors should consider four guidelines.

- *Understand the data.* Data can be an organization's most important asset, and internal auditors should understand both the data that is currently available in the organization and the data that is not available. This knowledge can help prioritize the types of analysis appropriate to the organization and to internal audit.
- *Prioritize acquiring data analytics skills.* Although every auditor does not have to be a data analytics specialist, every audit team should have at least one member who is data-focused and can spend a portion of his or her time on analytics. This person ideally should be technology-savvy and interested in how analytics can improve existing internal audit processes. Given the demand in the marketplace for data analytics skills, the ability to recruit and retain personnel with these skills will be an important investment and strategic decision for organizations.
- *Select the right tools.* Traditional audit analytics focuses on analyzing structured data through tools like Microsoft Excel and Access. With big data and analytics, more powerful tools are available for data visualization, statistical analysis, and business intelligence. These tools require additional training but can provide the mechanism for reaping the benefits of big data.
- *Develop a road map.* As part of the strategic planning process, the internal audit function should build a two- to three-year road map outlining a planned approach for incorporating analytics into the current internal audit processes. This plan will highlight the overall objectives of analytics in the audit processes, as well as the costs and benefits. While an organization initially might focus on data analysis to better understand past events, data analysis also can evolve to predictive analytics, where data is used to make predictions of future events. With a road map, the objectives of analytics can be linked directly with the data maturity of the organization, as well as with the internal audit function's objectives.

Tool for Transformation

Following the four data analytics guidelines can potentially transform the internal audit function. By analyzing the organization's data more strategically, auditors can better understand the organization and gain additional insights from the data. The data can be used for supporting the financial statement audit, as well as improving efficiency within the organization. For example, an auditor can examine 100 percent of travel expense data to provide more evidence of the accuracy of the expense accounts, test for fraudulent transactions, and test the relevant controls.

From a risk management perspective, data trends and anomalies can provide insights into the risks facing an organization. An emerging area in risk management is the use of unstructured text analysis to examine large amounts of *text-based artifacts*, perhaps from social media sites, to detect word patterns that could indicate potential risks to an organization.

Big data and data analytics provide an opportunity for internal auditors to perform truly data-driven audits. By prioritizing data analytics, internal auditors can harness big data and increase their overall value to the organization.

LORRAINE LEE, PHD, CPA, CISA, *is an associate professor of accounting at the University of North Carolina-Wilmington.*

Risk Watch

BY PAUL SOBEL

IS INTERNAL AUDIT IN YOUR AUDIT UNIVERSE?

The activity should be subject to the same objective assurance as other valuable, risk-oriented functions.

At the start of a recent presentation, I asked a group of internal auditors to stand up if they thought internal audit was of great value to their organizations. Not surprisingly, everyone in the room stood up. I then asked them to sit down if they thought it would be acceptable if internal audit underperformed. Nobody sat down. Finally, I asked them to sit down if they thought other corporate functions that were just as valuable as internal audit should be audited periodically. Everyone sat down.

The purpose of this exercise was to demonstrate that an internal audit activity, if truly delivering the level of value it is capable of delivering, should be subject to an independent review. Because internal audit is an important part of an organization's processes to assess and monitor risk management activities, failing to get assurance on internal audit's effectiveness may diminish the organization's overall risk management effectiveness.

The Audit Universe

An audit universe is a list of all auditable entities in an organization. An auditable entity could be a location, department, function, financial statement area, compliance requirement, or a multitude of other entities. Including such an entity in the audit universe is justified if the entity has some role in creating or preserving value for the organization. Stating it differently, an auditable entity has some role in managing one or more risks to the achievement of organizational objectives. If it can't be tied to an objective and risk, it shouldn't be in the audit universe. The auditable entity's role in managing those risks could be a form of risk mitigation such as controls, risk seeking—helping the organization take on or exploit risk to its advantage—or monitoring some aspect of those two.

The International Professional Practices Framework's new mission for internal auditing includes the phrase, "to enhance and protect organizational value." That mission aligns with the description of auditable entities. Most internal audit activities follow a risk-based approach, which helps them deliver on that mission. The Glossary to the *International Standards for the Professional Practice of Internal Auditing* (*Standards*) defines *risk* as "The possibility of an event occurring that will have an impact on the achievement of objectives."

Therefore, any organizational activity that helps to reduce the impact or likelihood of negative events (protect value) or increase the likelihood that objectives will be achieved (enhance value) should be included in the audit

SEND RISK WATCH ARTICLE IDEAS to Paul Sobel at paul.sobel@gapac.com

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

universe. This logic supports including the internal audit activity in the audit universe.

A Quality Assurance Review

The Glossary to the *Standards* defines *assurance services* as "An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization." Broadly, an assurance-focused audit typically involves:

- Establishing one or more objectives for the audit such as determining the accuracy of financial reporting or certain recorded amounts, evaluating the adequacy of internal controls, confirming compliance with laws and regulations, or assessing the effectiveness and efficiency of certain processes.
- Understanding criteria against which an examination can be made. For example, such criteria may be generally accepted accounting principles for a financial reporting audit, regulations or policies for a compliance audit, or leading practices for a controls-focused or operational audit.
- Gathering evidence to support judgments and conclusions as to how effectively the area being audited is achieving those audit objectives and the associated criteria.
- Reporting on the results of the audit.

The means to audit an internal audit activity is through a quality assurance review. The interpretation to Standard 1300: Quality Assurance and Improvement Program states, "A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the *Standards* and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement." That interpretation provides the outline for conducting an assurance review of the internal audit activity. The objectives of a quality assurance review are to:

- Evaluate the internal audit activity's conformance with the *Standards*.
- Evaluate whether auditors apply the Code of Ethics.
- Assess the efficiency and effectiveness of the internal audit activity.
- Identify opportunities for improvement.

The criteria are the *Standards* and the Code of Ethics. Evidence is then gathered to support achievement of those objectives and, more specifically, conformance with the principles and requirements outlined in the *Standards* and Code of Ethics. Finally, a report on the results of the assessment is issued to communicate the results of the assurance engagement.

There's one final requirement to truly make it an audit of the internal audit activity: an objective examination of evidence. Self-assessments and other forms of review can be an important part of a quality assurance and improvement program, as outlined in the *Standards*. However, to live up to the level of other internal audits, a quality assurance review should be conducted by individuals who are objective, such as appropriately trained individuals from a peer company or an outside service provider. This objective party should report on internal audit's conformance with the *Standards* to the appropriate stakeholders. Once these final requirements are met, the CAE can feel comfortable that an audit of the internal audit activity has been completed.

Don't Be Left Standing

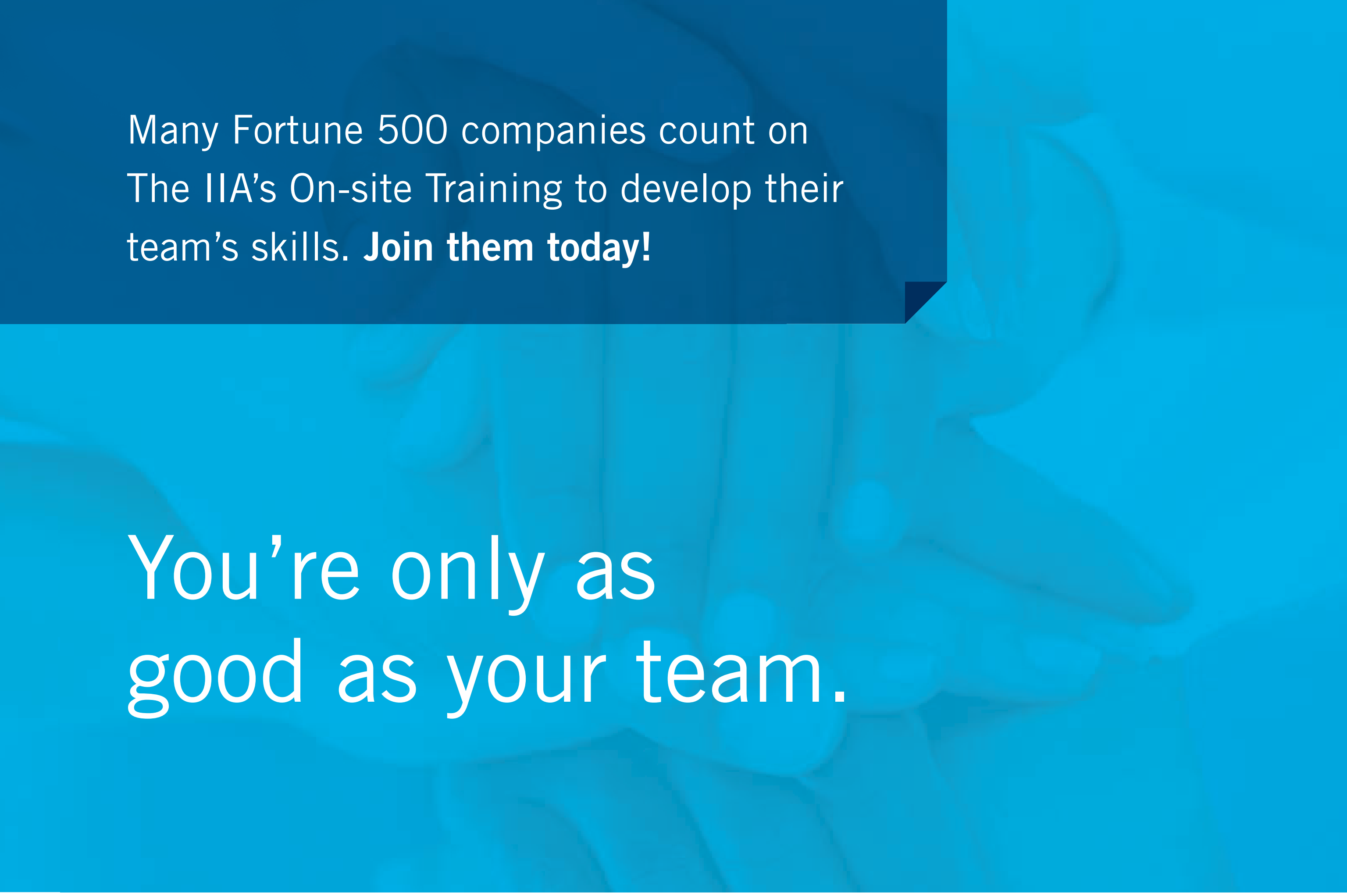
It should be clear that if an organization's internal audit activity is truly valued and plays an important governance role, it meets the criteria for being an auditable entity that should be included in an audit universe. Once internal audit is part of the audit universe, a risk-based approach should be applied to determine how often it should be audited, although to comply with the *Standards*, the audit should be performed at least once every five years.

The steps to perform such an audit are well-documented in the quality assurance review approach, which aligns with internal audit's assurance service approach. Finally, the quality assurance report should be sent to key stakeholders, just like any other audit report is. If there are gaps in performance, the CAE should provide an action plan to close those gaps to internal audit's key stakeholder, the audit committee.

This all seems logical and rooted in the *Standards*, yet only 42 percent of respondents to the 2015 Global Internal Audit Common Body of Knowledge Practitioner Survey indicate they conform with the 1300 series of the *Standards* related to a quality assurance and improvement program. It's up to all internal auditors to make sure that if they're ever asked to stand up in a crowd if they think internal auditing is important, and then sit down if their internal audit activity is audited, they aren't one of those who remain standing. Ia

The CAE should provide an action plan to close gaps in performance.

PAUL SOBEL, CIA, QIAL, CRMA, *is vice president and CAE for Georgia-Pacific LLC in Atlanta.*



BY BRYANT RICHARDS

BLURRED LINES

Internal auditors need to have the skills and perspective to deal with frauds that don't match the standard villain story.

Peter Singer, the head of a marketing department at an event company, was retiring but agreed to stay on for six months to transition the new department head. On day two of the transition, the incoming department head called the CAE and left a voicemail message saying something odd was going on and urged him to take a look.

During the investigation, the CAE found that Singer purchased marketing services from a vendor to support revenue targets for a specific product. Although that seemed reasonable, the audit also revealed that Singer was holding US$500,000 in late invoices from the vendor, a significant amount to the company. Some invoices were overdue by 18 months, well past the typical 45-day average pay cycle. The vendor representative sent numerous emails to Singer complaining about the invoices.

The invoices were being paid increasingly late beginning several years earlier, when the budget for this marketing service was reduced by US$400,000. This was due to the belief that the vendor's services were less useful as the product became more established in the marketplace. If the invoices had been paid timely, Singer would have been over budget. The invoices were never sent to accounts payable, as Singer asked the vendor to send the invoices directly to him. In addition, Singer never disclosed these commitments during the monthly financial close process.

Singer sent emails requesting that the vendor reduce the amounts of the invoices so that he could avoid additional approvals. The vendor complied by splitting invoices. Singer also developed a close personal friendship with the vendor representative—they would often go on trips together with their spouses. They were so close that, when Singer's wife lost her job two years earlier, the vendor representative offered her a position at his firm.

As seemingly fraudulent events like this are investigated, internal auditors are often quick to look for the motivations and benefits to the perpetrators. Although the situation unraveled with a lot of juicy, and often irrelevant, tidbits of information along the way, management wanted internal audit to focus on one question: Why did Singer do it?

After hundreds of hours of research and several hours of interviews, internal audit was left with a troubling assessment of Singer's behavior. He had committed fraud. He lied to the company about spending money with the vendor by making it appear that he was on budget, evidenced by the outstanding invoices. He was aware of these outstanding invoices, as they

SEND FRAUD FINDINGS ARTICLE IDEAS to Bryant Richards at bryant_richards@yahoo.com were piled up on his desk. He worked hard to circumvent internal controls for authorizing and recording the invoices, and the vendor representative conspired with him to circumvent company authorization limits. Because of this activity, the company had a US$500,000 debt for services it did not authorize, value, or want.

Internal auditors are often quick to look for the motivations and benefits.

In the end, there was no direct and convincing way to prove that Singer received any benefit from the vendor. In the eyes of management, this made the behavior much less grievous and "not quite fraud." Internal audit was able to convince management that Singer intentionally circumvented internal controls to conceal the budget overrun, so he was asked to leave a few months earlier than planned. Consequently, management changed the policy to have all invoices sent directly to accounts payable to avoid future errors. However, management paid the outstanding invoices without confronting the vendor about its part in knowingly evading internal controls.

The absence of a clear-cut villain stealing from the company left management wondering what the concern was about. As a result, management sent a muddled message about what is acceptable and missed an opportunity to strengthen the company's defenses against future fraud.

Fraud investigations are often the most intriguing part of an internal auditor's job. You have villains, who break rules and selfishly benefit to the detriment of the organization. Until someone catches on, that is.

However, the reality is not always so clear cut. In fact, it could be argued that the villain situation is rare. In many cases, a confused individual takes a few small steps across the line of good judgment and winds up entangled in rationalizations and good intentions. As things progress, this person hears the chirping of his or her conscience that something isn't right, but the warning is distant and the words are muffled. In the end, the employee is baffled as to how his or her actions were perceived so negatively. The individual knows he or she could have done things better, but can't believe the situation is being taken so seriously. Termination? Fraud? The employee is shocked by the possibility, and many times will utter the words, "But I didn't steal."

It is always difficult to see ordinary people fumble into bad situations. And organizations are not always prepared to handle these situations, which leads them down a messy road of uncomfortable conversations, half measures, and lackluster support.

Lessons Learned

- Organizations need to establish a clear perspective on how they want to approach fraud and its many faces. A strong fraud policy describes what the company perceives as fraud and lays out the expectations for investigation and resolution. Without a policy, fraudulent activity is often addressed by management based on the biases and perspectives associated with each unique instance.
- Internal audit should use these situations to improve the organization's fraud perspective. Fraud is often interpreted and managed differently across organizations based on corporate culture and understanding of internal control. Although frustrating for those involved, management's lukewarm support may be the most valuable observation from this scenario. It is an indication that there is significant work to be done to improve internal control awareness at the top of the organization.
- Internal audit has the expertise, perspective, skills, and independence to lead in these situations. Expecting others to share a clear vision of murky fraud cases is not always realistic.

BRYANT RICHARDS, CIA, CRMA, CMA, *is an associate professor of accounting and finance at Nichols College in Dudley, Mass.*

INTEGRATED REPORTING

Taking the Lead on Nonfinancial Reporting

Internal audit is well-positioned to examine how its organization reports on nonfinancial issues.

Arthur Piper

Illustration by Sean Yates

By December, governments across Europe will need to have translated the European Union's (EU's) 2014 Directive on nonfinancial reporting into their national rule books. Formulated in response to the perceived short-termism that contributed to the global economic and financial crisis in 2007, the rules mandate that Europe's top 6,000 companies disclose in their annual report and accounts how they are discharging their social, environmental, and ethical duties.

60
70
P
R
O
OC
±50
6ΔU
PH
±1/2
O
RL
RMH
RMV
±0.25
.25

"Disclosure of nonfinancial information is vital for managing change towards a sustainable global economy by combining long-term profitability with social justice and environmental protection," the 2014 Directive says. "In this context, disclosure of nonfinancial information helps the measuring, monitoring, and managing of undertakings' performance and their impact on society."

Who benefits most from this additional reporting burden? Nicolas Bernier-Abad—who is in charge of seeing the rules come to fruition at the European Commission's Directorate General of Financial Stability, Financial Services, and Capital Markets Union—told internal auditors at a recent event organized by the European Confederation of Institutes of Internal Auditing in Brussels that nonfinancial reporting was "pro-business." "The aim is not to create a new report, but to add content to the existing management report regarding environmental and social obligations, action to counter corruption and bribery, and in respect of human rights," he said. He added that for executives and boards to understand what is going on in their own organizations, these issues had to be spoken about in the same way as one would talk about profit and loss.

The Directive will be the biggest compulsory reporting project of its kind.

While an estimated 2,000 companies in Europe already produce and use such information, the new Directive will set in motion the biggest compulsory reporting project of its kind. It is likely to help standardize what has been a growing trend globally during the past 10 years. The movement to provide more comprehensive reporting on matters that do not fall under the financial reporting remit has gathered steam under a range of titles—such as integrated reporting, corporate social responsibility reporting, and sustainability reporting—but thus far there is no agreed-upon approach or methodology to capture these disparate topics under a single reporting framework or set of standards.

A MORE SERIOUS DOCUMENT

European internal auditors who have been involved in developing nonfinancial reporting mechanisms tend to agree with Bernier-Abad's assessment. While the reports do give investors, environmental pressure groups, and others a larger and more detailed window into the business' operations, management also wins.

"In general, if you look at the development of sustainability reports in companies, there is a move away from producing a marketing document and toward producing a much more serious document where the company discloses how they perform in certain areas," says Mark Jongejan, vice president, Group Internal Audit at the Danish brewer Carlsberg.

Internal audit not only assesses the accuracy of the specific key performance indicators to be disclosed in the report but has helped build an awareness within the company about the relevance of this type of reporting. "To be able to develop good strategies, you need reliable data," he says. "The internal audits we performed in this area have enabled us to have discussions with management on how you organize the whole governance process around nonfinancial reporting, the roles and responsibilities needed, what kind of tools to deploy, and how you train your people in the organization."

In the beverage industry, one big challenge is how to reduce water usage. "To be able to develop a good strategy and to set clear objectives for the coming three to four years, you have to know where you are at this point in time," he says. "You need accurate data. You need good nonfinancial reporting systems."

While the EU Directive is making nonfinancial reporting the norm for European companies like Carlsberg, there has been less pressure in the U.S. to go down this route, not least because the Sarbanes-Oxley Act of 2002 focused many businesses and their internal auditors on providing assurance primarily around financial controls. But that does not mean U.S. auditors are not engaged in such projects.

"Outside of the many U.S.-based multinational companies that are talking about this, the terminology really hasn't caught on here yet," says Jim Pelletier, IIA vice president, Professional Solutions. "Auditors who are taking a risk-based approach and are looking at the major objectives of the organization are likely to be hitting these areas—they're just not calling it the same thing."

Pelletier says the focus on nonfinancial reporting also marks a turn away from providing assurance on the traditional, historical performance of the company, to a view that looks ahead at the potential big risks that could impact the organization. Given the range and variety of risks that pose a threat today, it makes sense that many of those are nonfinancial in nature. In that sense, nonfinancial reporting is an acknowledgement that risk-based auditing has a crucial role to play in the long-term success of each organization.

INTEGRATED THINKING

Silvio de Girolamo, group chief internal audit and corporate social responsibility officer at the food and beverage group Autogrill in Milan, Italy, is a contributor to the 2015 IIA report, Beyond the Numbers–Internal Audit's Role in Nonfinancial Reporting. He says in many organizations—his own included—nonfinancial reporting has proved its worth to management in specific areas and has grown in stature from this success.

His experience at Autogrill mirrors that of Jongejan's at Carlsberg. "When you begin to measure what is happening in these areas, you can start to manage those processes that you did not manage in the past and improve on them," de Girolamo says. But there is an opportunity for internal audit to play a defining role in how nonfinancial reporting is to be developed because of the lack of prescription on how it should be implemented.

"Internal auditors can play a defining role by becoming change agents within their businesses," he says. He accepts the move into these areas is a challenge for internal auditors, given their traditional focus on financial controls, but is confident that the profession can help promote integrated thinking in the businesses they serve.

"We need to argue that the company has to put in place a methodological approach to manage these areas, not just as a collection of individual problems, but as something more integrated and interconnected," de Girolamo says. That involves a recognition of the importance of the organization's social role and impact, and a proactive way of seeking out effective solutions that are good for both the company and its stakeholders.

"Auditors who are taking a risk-based approach and are looking at the major objectives of the organization are likely to be hitting these areas."

Jim Pelletier

Internal audit is positioned to achieve this objective—what he calls integrated thinking—because it can take a helicopter view of the entire organization that could help it move from dealing with its social reporting in an ad hoc manner to something more holistic. But he also admits that not all CAEs will be in a position to jump to this higher level of operation immediately.

"Internal audit's role depends very much on the maturity level of the company in nonfinancial reporting," he says. Internal auditors can perform an advisory role or an assurance role—or something in the middle. That can entail supporting management in understanding which kinds of reporting systems are going to be most effective, helping it improve those systems, or providing assurance when they are well-established.

RISE TO THE COMPETENCY CHALLENGE

The role is not without its challenges. The most important of these is filling the competency gaps within internal audit, itself, according to Mentes Albayrak, audit coordinator at the Turkish conglomerate Anadolu Group and IIA–Turkey vice chairman.

He says auditors have two kinds of competency: process and content competencies. "Internal auditors have the right process competencies for effective nonfinancial reporting, such as the ability to communicate with stakeholders, extensive knowledge of how to perform an assurance engagement, and knowing the *International Standards for the Professional Practice of Internal Auditing*," he says.

But there are differences in the way internal auditors need to apply these competencies when it comes to nonfinancial data. While auditors have the information and knowledge about how to decide on materiality when it comes to financial controls,

"The company has to put in place a methodological approach to manage these areas, not just as a collection of individual problems, but as something more integrated and interconnected."

Silvio de Girolamo

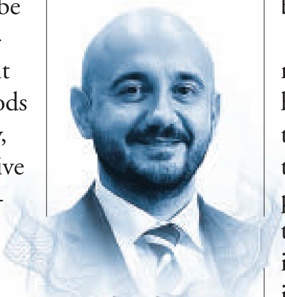
for example, the issue of materiality for nonfinancial controls also entails reaching out to stakeholders.

"Internal auditors need to understand what information is relevant to the business' key stakeholders, and understand what is significant to them and how much it matters," Albayrak says. "Unlike deciding materiality on financial controls, this involves exercising a much greater degree of professional judgment."

Decisions on materiality over nonfinancial reporting issues should be systematic, transparent, and accountable. "That means when management or stakeholders ask about your methods or systems of determining materiality, you have a system in place and can give a comprehensive answer to that question," he says.

That requires a more outward-looking approach—one that entails internal auditors reaching out to their stakeholders and engaging in communication. For auditors who have been focused largely on financial controls, that could be a big shift in emphasis. Nonfinancial reporting requires auditors to understand the finer points of communication. When it comes to working on issues such as culture, auditors are asking people to share their opinions and feelings—rather than merely collating facts and figures, says Tea Enting-Beijering, one of several CAEs within the Netherlands' Central Governmental Audit Services directorate within the Ministry of Finance.

"When we started our nonfinancial auditing project, we selected auditors who already had strong communication skills, and we invested in more education for them," says Enting-Beijering, who is CAE for the Ministry of Infrastructure and Environment. She selected a handful of people out of the 600 auditors on the team. Her objective was to look at the organization's culture because the standard financial audits could not pick up on how changes to its working practices were impacting the business.



"[Internal auditors] need to establish the information on which to provide assurance, but we can't have competency on the content of all areas."

Mentes Albayrak

Developing good listening skills and creating an atmosphere with the right level of intimacy and trust was key. "If there is not enough trust, it is difficult to get people to share their opinions and feelings," she says. Communicating the audit findings with those involved also needed to be handled with sensitivity because people need to feel they have been listened to and their concerns have been taken seriously.

She says the audits have given managers a much clearer picture of how their work fits into and impacts the wider ministry. It also has helped the audit team provide advice on how processes can be improved and how things can be done better. "The most important thing is that we are now having conversations in the organization that are very good and are leading to real change," she says.

"The most important thing is that we are now having conversations in the organization that are very good and are leading to real change."

Tea Enting-Beijering

While communication is key, Albayrak says, the biggest challenge in filling internal audit's competency gap is in what he calls content competency. "In nonfinancial reporting, you'll have environmental issues, ethical issues, noneconomic issues, and sometimes macroeconomic issues that form the content of the report you are working on," he says. "It isn't possible for an internal auditor to know everything. We need to establish the information on which to provide assurance, but we can't have competency on the content of all areas."

Albayrak's solution is similar to de Girolamo's: Provide integrated assurance, or combined assurance, by creating a multidisciplinary team of experts from across the organization and beyond. If no party has the full spectrum of competencies required to provide assurance on nonfinancial reporting, then the various parties involved in this assurance process should be coordinated effectively.

32% of CBOK respondents' organizations have combined assurance activities, notes the Internal Audit Foundation's Combined Assurance: One Language, One Voice, One View report.

"Internal auditors are best positioned to provide that coordination," he says. "We have the process competencies, we have the general outline of what content competencies are needed, and we have a general knowledge from the work in our own organizations about what environmental, human resources, social, and ethical issues the business faces."

That gives internal audit the ability to form an effective, multidisciplinary team, coordinate that team, and get the input needed from management, or external consultants, to ensure all of the relevant technical content goes into the process. A 2015 paper, Combined Assurance: One Language, One Voice, One View, written by Sam Huibers and published by the Internal Audit Foundation's Global Internal Audit Common Body of Knowledge (CBOK) research project, outlines how this approach can bring disparate parties together to provide a single statement on assurance that unites their perspectives. But while two out of three European organizations taking part in the 2015 CBOK practitioner survey said they were aware of this approach, just over half (53 percent) of North American respondents said they were—below the 59 percent global average.

CREATE A CONSISTENT APPROACH

The headline figures emerging from the CBOK study may be more a matter of semantics. Just as some U.S. internal auditors are engaging in many of the areas that in Europe go under the heading of nonfinancial reporting, so does The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2013 *Internal Control–Integrated Framework* provide support for those working in this area, says COSO Chairman Robert Hirth. Every U.S. stock exchange-listed company uses the framework to comply with Section 404 of the Sarbanes-Oxley Act of 2002, covering internal control over external financial reporting. "But all forms of reporting are a specific control objective area in the COSO framework," Hirth says, "and that reporting is defined as being internal, external, financial, and nonfinancial reporting."

The aim is to create a consistent approach and common language for evaluating all forms of internal control and all forms of reporting, he says. That requires CAEs who are implementing nonfinancial reporting to start at the top. "Get management and, as needed, board and audit committee buy-in and agreement that validating this nonfinancial reporting is valuable, desired, and makes sense against other priorities and resource constraints—some companies have a lot of resources, others have very little," he advises.

Next, identify the most critical, important nonfinancial reporting that should be validated and audited. "This means that there will likely end up being lots of nonfinancial reporting that doesn't make the cut—at least for now," Hirth says. "Determine which internal and external information falls into scope." For example, internal reporting on diversity or employee evaluations may be important and external reporting on sustainability or corporate social responsibility may also be just as important. CAEs need to include all of those critical areas in their plan.

Finally, he says, internal audit needs to involve and engage the first line of defense processes and people who produce the reporting information. "Also, look at how you can leverage information systems to generate the information with a higher level of accuracy and integrity, and try to eliminate the manual production of this information," he advises.

CONQUER THE BIG STUFF

There are likely to be a few sticking points to audit involvement in nonfinancial reporting, particularly defensiveness among those people preparing the reports, as they may never have had their work challenged or audited in the past. "Deal with this professionally, but don't back down if the information is truly important," Hirth says. In addition, there may be a lack of controls related to the reporting involved, and internal audit's main role in that case is to identify the important gaps. "There's a danger of doing work on information that doesn't really matter," he says. "Don't chase the little stuff. Chase and conquer the big stuff."

People preparing nonfinancial reports may never have had their work audited.

The need to boost their skills, competencies, and even head count in this area is a huge challenge ahead for the profession. In addition to creating audit departments that are more risk-based, forward-looking, and willing to reach out to stakeholders, they also will have to work more collaboratively than ever to succeed.

Worried? De Girolamo isn't. He thinks nonfinancial reporting will be the next catalyst to grow both the stature and size of the internal audit profession. "It's a big challenge for sure, but one internal audit is more than ready to meet," he says. Ia

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

Ia
INTERNAL AUDITOR
BE THE
FUTURE
Win a US$1,000 Scholarship

COPYRIGHT © BOEING

Audit processes *take flight*

The updated COSO *Internal Control–Integrated Framework* is at the heart of Boeing's internal audit work.

Tim Boyle
Dennis Applegate

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) revised *Internal Control–Integrated Framework* offers internal audit departments an opportunity to take a fresh look at their processes for evaluating internal control. For the internal audit function at The Boeing Co., the release of the 2013 update has been the catalyst for adding more discipline and structure to its work.

The updated framework's most significant new development is that it codifies 17 guiding principles that articulate the concepts underlying the five control components described in the original version: control environment, risk assessment, control activities, information and communication, and monitoring activities. Moreover, it adds 77 explicit points of focus spread across those principles to assist users in understanding the structure of a well-designed and effective internal control system. The framework now also requires organizations to use the principles to assess the effectiveness of internal control, although it allows management to determine the suitability of the points of focus.

COSO's revised internal control framework became its authoritative framework at the end of 2014. By 2015, Boeing Corporate Audit had updated its audit process, ensuring that its internal auditors consistently tested each control component and exercised sound judgment in determining whether all five components were *present* and *functioning*, and *operating together,* as articulated in the 2013 framework.

PRINCIPLES-BASED APPROACH

Boeing develops and executes a risk-based audit plan aligned with key business objectives. As a manufacturer of commercial and defense aerospace products, its audit plan primarily focuses on operational objectives such as the development of new airplane designs, management of suppliers—including procurement of major parts and assemblies such as engines and landing gear—and the production and testing of commercial and military aircraft. Such audits are generally not focused at the entity level, but rather on processes at the division, plant, product line, or functional level. For that reason, assessing all 17 principles on every audit would not add value for most audit clients. Instead, Boeing's internal auditors apply a subset of the COSO principles tailored to ensure that audit adds value on all engagements.

Audit management and staff brainstormed and documented the new COSO-based audit criteria using the principles and points of focus supporting the five COSO control components, but they adapted them to Boeing's environment (see "COSO Evaluation Considerations for Auditors" on page 38). This guidance has driven a consistent implementation of the 2013 framework, making it relevant and value-added to both auditors and clients, alike. Moreover, the criteria have compelled audit testing of all COSO control components for sufficiency, not just control activities. Auditors tend to focus the bulk of their control testing on the COSO control activities component because it is the component traditionally containing the preponderance of controls at the process-level. However, giving audit attention to all COSO components provides a more comprehensive evaluation of significant risk, better serving client management.

Because the 2013 framework cautions that the use of principles or points of focus are not meant to imply a checklist, Boeing's Corporate Audit staff is trained and empowered to exercise judgment in determining the nature and extent to which the criteria are applied. Yet they must take care to keep the focus always on inherent risk. The guidance on COSO principles and points of focus, coupled with the endorsed audit evidence, form the criteria that assist the company's internal auditors in assessing whether the components of internal control are present, functioning, and operating jointly.

AUDIT DOCUMENTATION

To back the new COSO-based approach, Boeing Corporate Audit developed a condensed and integrated audit template for documenting all relevant facts and data used to evaluate each COSO control component. It includes the guidance from the COSO Evaluation Considerations and requires auditors to document what was evaluated in the control design assessment phase and what was tested in the operational assessment phase, including the conclusions reached for each component. It also mirrors certain aspects of the traditional risk and control matrix that should be familiar to most internal auditors. This "extended risk control matrix" (E-RCM) is a required audit workpaper for each process objective in Boeing's internal audit protocol and provides audit management a point of departure in due diligence reviews of the audit work performed, a quality assurance step designed to comply with IIA Standard 1311: Internal Assessments.

In the preliminary survey phase of the audit, the E-RCM serves two key purposes. First, it shows the alignment of process controls to the related COSO control component. Second, it allows the internal auditor to document potential control gaps and to indicate whether the alignment of controls provides sufficient risk coverage.

In the fieldwork phase, auditors document the testing of the defined controls for design and operating effectiveness in separate columns of the E-RCM. Such documentation provides support for the auditor's opinion on the discrete controls and how those controls may or may not support the components as being present, functioning, and operating together.

Moreover, every audit requires a detailed process flowchart. Confirmed with client management, the flowchart details the movement of activities and documents through the process, and identifies key control points requiring audit examination. Many audit professionals use process flowcharts to define and document their understanding of the audit subject. The same purpose is served in Boeing's COSO-based audit process, though the process flowchart has taken on an extra dimension as the initial basis for the E-RCM.

96% of companies reviewed in fiscal year 2015 have adopted the 2013 COSO *Internal Control–Integrated Framework*, according to an analysis by Audit Analytics and Protiviti.

The key elements of the revised audit process, as reflected in the E-RCM, are:

- *Process objective.* Derived from relevant company policies and procedures, industry standards, or other business goals and confirmed with client management before an audit begins.
- *COSO components.* Each discrete control to be assessed as part of the audit is grouped with the component to which it is most closely aligned. The results of the control assessment are then used to support the evaluation if that component is present and functioning in support of the process objective. If no specific controls are associated with a component, then the component is still evaluated through inquiry, observation, and inspection, as needed.
- *Inherent risk.* Documents negative events and their effects on achieving the predetermined process objective in the absence of management controls.
- *Controls.* Describe the attributes of each risk-mitigating control, including *who* is responsible for the control, *how* and *when* control execution is accomplished, *what* is involved in executing the control, and *why* it is important.
- *Control design assessment.* Documents how each control was assessed for design effectiveness, the results of that testing, which of the various controls are key, and whether those controls are present to achieve the objective. This control testing, along with the process-level evaluation, supports the overall opinion on whether the COSO components are present and working together.
- *Operating effectiveness testing.* Documents the results of audit tests of control operation, emphasizing the use of audit sampling techniques to determine whether the controls are functioning as designed.
- *Conclusion.* Summarizes the auditor's determination of whether each of the five components is present, functioning, and operating together as a unit to provide reasonable assurance of achieving process objectives.

The updated audit process provided an opportunity for increased discipline in defining processes, risks, and controls.

THREE KEY ELEMENTS

Although the elements of business processes, risks, and controls have been a focus of Boeing's internal audit work for many years, the updated audit process provided an opportunity for increased discipline in the definition and alignment of these three key elements.

Process Objectives In Boeing's revised audit process, auditors issue an opinion to client management on whether the COSO control components are present, functioning, and operating together in support of the stated process objective, pursuant to the 2013 framework. Typically, a process objective will fall entirely within operations, reporting, or compliance—the basic objective categories defined by COSO—but occasionally it may cover more than one COSO objective.

The E-RCM documentation supports each assessment by component and provides a clear line of sight from

continued on page 40

COSO EVALUATION CONSIDERATIONS FOR AUDITORS

CONTROL ENVIRONMENT

1 Are the responsibilities, accountabilities, and authorities (RAA) established and communicated effectively through policies, procedures, or other methods to support process and control objectives?

- Are control performers' responsibilities aligned with authority or accountability?
- Are organizational responsibilities identified (e.g., charter and structure) and people assigned to achieve the process objectives and key deliverables?
- Is there segregation of duties to mitigate misrepresentation or misstatement of operations (fraud risk)?

Potential Audit Evidence to Support Conclusions
Inspect organizational charts/charters and confirm that current job responsibilities are aligned with relevant process objectives.

2 Do control performers have sufficient competencies to execute controls?

- Do they understand the risk and objective of the control?
- Does the control performer have the experience/training necessary to execute the control?

Potential Audit Evidence to Support Conclusions
Evaluate results of control testing (as applicable) where competence is an attribute.

3 Are management actions and priorities consistent with stated objectives, RAA, and Boeing values?

Potential Audit Evidence to Support Conclusions
Evaluate whether management actions align with supporting process objectives (i.e., demonstrated allocation of resources, priorities are managed to stated objectives, and corrective actions are taken).

RISK ASSESSMENT

1 Is a risk assessment occurring on a regular basis for the process? It could be formal or informal, but it should be happening in some form by management.

Potential Audit Evidence to Support Conclusions
Attend meetings to observe where risks are identified, monitored, and actions are taken. Are stakeholders represented and is the frequency adequate to help with risk mitigation?

2 Are process objectives defined specifically enough to support identification of inherent risk events?

Potential Audit Evidence to Support Conclusions
Inspect process objective definitions to evaluate whether objectives are stated specifically enough to support risk identification (this may not be documented, so use inquiry as needed).

3 Are inherent risk events identified and assessed?

- Are internal or external business changes (e.g., regulatory, funding, market, business growth or reduction, and system changes) considered within the risk assessment?
- Is the risk assessment occurring frequently enough to capture these changes?
- Have key stakeholders been identified and are they involved in the risk assessment?
- Are nonconformances or negative trends captured and evaluated for inclusion in the risk assessment?
- Are potential fraud risks (financial or nonfinancial) identified and evaluated (e.g., a nonfinancial fraud risk such as metrics that are intentionally misrepresented to hide poor performance or risk (reported as yellow; when they are red))?
- Are risk tolerances established, (e.g., a 2 percent error rate for manufacturing defects).

Potential Audit Evidence to Support Conclusions
Inspect identified risks for completeness of events (this may not be documented, so use inquiry as needed). Inspect metrics for negative trends and inclusion in risk assessment for systemic issues.

4 Has management determined appropriate risk response (i.e., accept, avoid, reduce, or share)? (See Control Activities.)

Potential Audit Evidence to Support Conclusions
Inspect control implementation as documented in policies and procedures, business process instructions, desk instructions, or other methods to evaluate whether identified risks are adequately responded to with controls.

COSO-based internal control systems can meet "the challenges of an ever-changing business and regulatory environment," notes Adding Value With COSO from the Internal Audit Foundation.

CONTROL ACTIVITIES

1 Are the controls designed and operating effectively to achieve their objectives, to mitigate the risks, and support the process objective?

- Control testing of attributes using statistically relevant samples will be the primary way to evaluate control activities.

Potential Audit Evidence to Support Conclusions
Control test results will be the most influential data for conclusion.

2 Based on the evaluation of risk events inherent to the process, have corresponding controls been identified? (See Risk Assessment.)

- Are there enough controls developed and implemented to mitigate the risks in the process (i.e., preventive, detective, manual, general computing controls, and IT dependent as needed)?

Potential Audit Evidence to Support Conclusions
Inspect process guidance where controls are defined, such as relevant command media, desktop procedures, manuals, and monitoring. Do they align with identified risks?

3 Are controls defined, documented, and communicated (e.g., command media, desktop procedures, manuals, and training)? (See Information & Communication.)

Potential Audit Evidence to Support Conclusions
Inspect control documentation and communication to control performers for sufficiency. Factors to consider for level of documentation include complexity of controls, significance of risks, number of control performers, and turnover expected. Lack of documentation may or may not be a deficiency.

INFORMATION & COMMUNICATION

1 For affected stakeholders, is information identified, validated, documented, communicated, and reviewed to achieve process objectives such that control performers can execute consistently (i.e., process steps, process RAA, control RAA, control definitions and objectives, changes to relevant policies, procedures, risks, and new initiatives)? (See Monitoring Activities.)

- Is documentation sufficient to match the level of risk and complexity of control?
- Is there data identified to support monitoring of control performance?
- Are there open channels of communication both top-down and bottom-up?

Potential Audit Evidence to Support Conclusions
Inspect information and communication of other relevant information (i.e., business/process objective statements, command media, change notifications, and metrics) and assess whether it is disseminated to relevant stakeholders (i.e., control performers, process owners, and management/customers/suppliers). (See Control Environment.)

- *Inspect process documentation to evaluate adequacy to support consistent execution by the control performers. (See Control Activities.)*
- *Inspect controls for associated information used to monitor and evaluate whether there is sufficient and reliable information and communication to identify failures timely.*

MONITORING ACTIVITIES

1 Does effective monitoring of the internal controls of the process exist?

- Are metrics in alignment with objectives, risk tolerance levels, and controls?
- Are out-of-tolerance conditions consistently identified (i.e., red and yellow criteria; or methods of effectiveness identified)?
- Are corrective/preventive actions identified, approved, and tracked to completion?

Potential Audit Evidence to Support Conclusions
Inspect metrics in use to evaluate whether they are aligned to the key objectives and risks, and that there are clear criteria for identifying unacceptable conditions.

2 Are metrics validated and communicated to relevant stakeholders? (See Information & Communication.)

Potential Audit Evidence to Support Conclusions
Inquire and inspect how metrics are validated and communicated to stakeholders.

MORE VISIT InternalAuditor.org to view the extended risk control matrix, risk definitions, and control model used by Boeing's Corporate Audit department.

continued from page 37

the process objective through the risks, controls, tests performed, and data used for the final assessment. The structured nature of the revised audit process also helps ensure that the auditor judgment exercised in rendering an opinion about the control components is informed by relevant audit facts and data. Concentrating an audit on process-specific objectives improves auditor focus and efficiency, enhances client understanding, and helps guard against scope creep. More importantly, it avoids overstating the final audit opinion, limiting it to the scope of the process objective and what was actually tested.

Assessment of Inherent Risk The 2013 COSO framework contains a more detailed conceptual analysis of inherent risk, control risk, and risk tolerance than the prior version. In response to this new COSO emphasis, Boeing Corporate Audit has increased its focus on auditor understanding of risk management concepts and the appropriate exercise of auditor judgment when determining the nature and extent of inherent risk. In rolling out the COSO-based audit process, Boeing further emphasized not only the need to identify inherent risk in all audits but to avoid conflating this risk with control risk, a distinction that the new COSO framework also has addressed.

Boeing uses a COSO-inspired risk model in auditor training. The model contains abbreviated versions of the COSO definitions for inherent, control, and residual risks, and a simple equation to show the corresponding risk relationships to client management. Auditor understanding of client management's risk tolerance also has assumed greater importance in the new COSO framework, and that requirement has been built into the risk assessment procedure. Despite their subjectivity, these risk concepts become meaningful to the audit client when modeled into a heat map.

The Control Model To ensure consistency in ascribing a particular control to a given component, Boeing Corporate Audit established a control model based on the concepts contained in the 2013 COSO framework. The control model defines 28 specific types of controls segmented by COSO components that may be present in each process, irrespective of the process objective. Some of these control types may cover more than one component. For example, "review performance metrics" may address the control activities component if the metrics pertain to management supervision or address the monitoring component if the metrics pertain to reviews of the internal control system. These criteria have helped internal auditors identify relevant controls and classify them by the control component prescribed in the model. This has resulted in more consistent control definition and COSO alignment.

AUDITOR OPINIONS

Once the audit and supporting E-RCM documentation have been completed and approved, Boeing Corporate Audit summarizes the evaluation of each control component and issues to the client an overall opinion about the health of the internal control system governing the process. Three kinds of opinions are possible:

- » The internal control components were determined to be present and functioning, even though some low-impact audit findings may be present.
- » The internal control components were determined to be present but not functioning.
- » The internal control components were determined to not be present.

Each deficiency is documented in a finding that then requires a corrective action by management. The rationale for any adverse opinion and the impact of significant process errors or omissions are detailed in the accompanying audit report.

TANGIBLE RESULTS

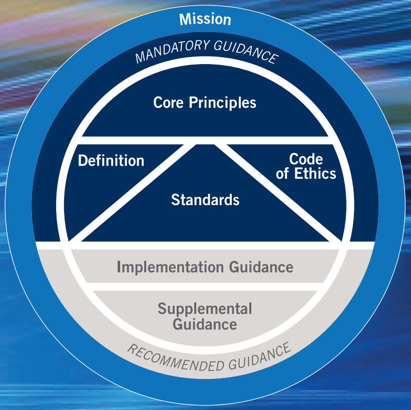
Since adopting this model with an emphasis on inherent risk, Boeing's internal auditors have increasingly targeted control design improvements for management attention, resulting in a 61 percent increase in the number of audit findings related to control design. Such findings tend to provide more value to audit clients because they improve the quality of the overall internal control system rather than improve the execution of specific controls within a system that is poorly designed.

The documented process improvements at Boeing support the proposition that COSO-based auditing yields an effective audit result. Specifically, testing all five COSO control components and related principles using a consistent baseline of COSO criteria and control types provides a solid foundation for determining the level of assurance provided for the objectives being evaluated.

Adopting a COSO-based approach to internal auditing has aligned the Boeing Corporate Audit process with a key professional standard. While the path to adoption is not easily navigated, internal audit departments willing to make the journey will be rewarded by more thorough audit coverage.

TIM BOYLE, CIA, PE, *is senior audit manager at The Boeing Co. in Seattle.*
DENNIS APPLEGATE, CIA, CPA, CMA, CFE, *is an adjunct professor at Seattle University.*

IPPF International Professional Practices Framework



Latest Guidance Released From The IIA!

Free Downloads for IIA Members!

As part of The IIA's International Professional Practices Framework® (IPPF®), **Implementation Guidance** assists internal auditors in applying the *Standards* and **Supplemental Guidance** provides detailed processes and procedures for internal audit practitioners.

Implementation Guides

- Implementation Guide 1010: Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter
- Implementation Guide 2500: Monitoring Progress
- Implementation Guide 2600: Communicating the Acceptance of Risks
- Implementation Guide: 1100 Series — Independence and Objectivity

Supplemental Guidance

Global Technology Audit Guide (GTAG)

- Auditing Smart Devices: An Internal Auditor's Guide to Understanding and Auditing Smart Devices
- Cybersecurity: A Practitioner's Guide to Assessing Cybersecurity Risk

Interested in becoming a Global Guidance Contributor? Visit the website to learn more about our Volunteer Global Guidance Contributor Program.

*Nonmembers may purchase IIA Standards and Guidance publications online through The IIA Bookstore.

Visit www.theiia.org/newguidance to download new guidance from The IIA.

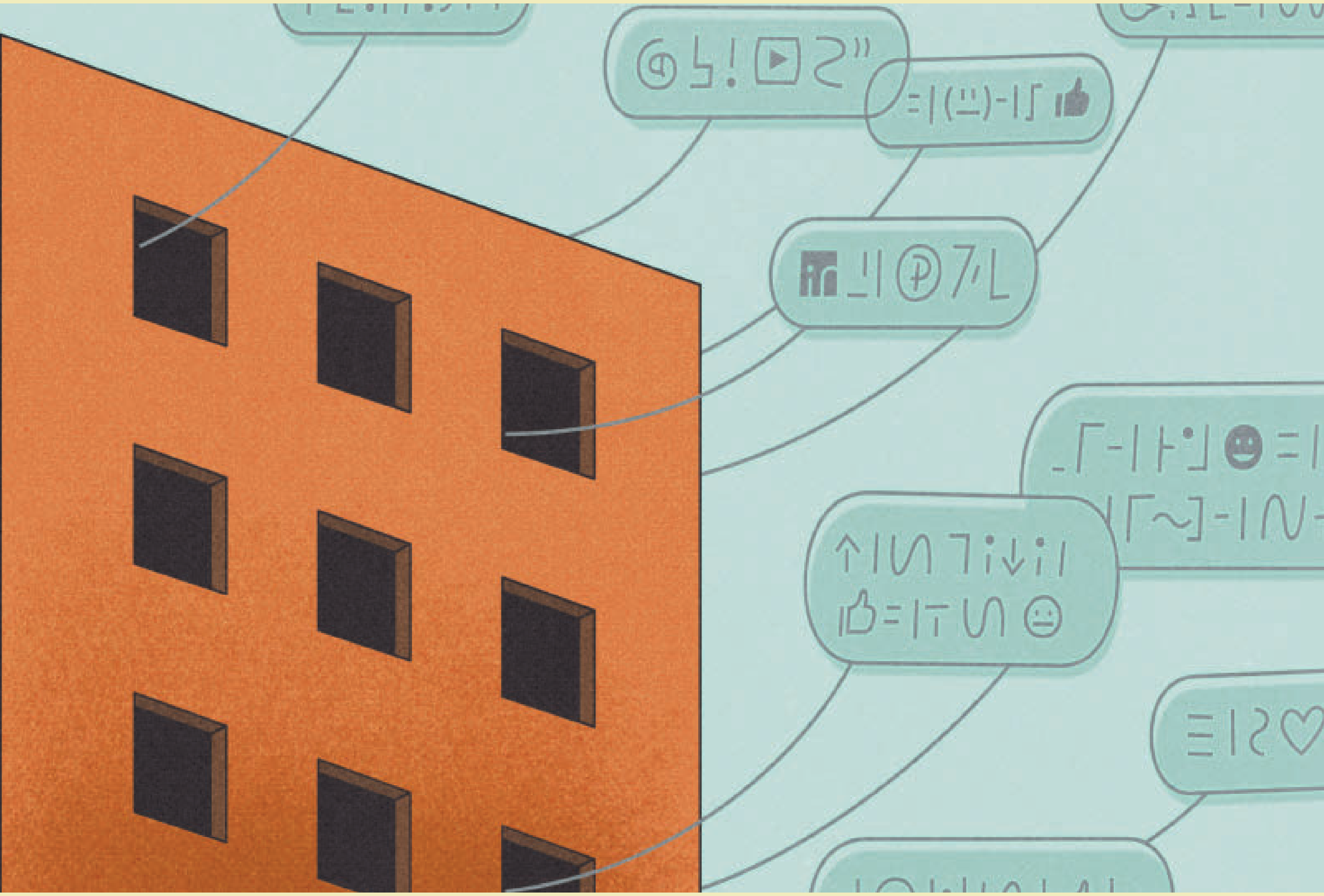
75TH ANNIVERSARY 1941-2016

IIA® The Institute of Internal Auditors

2016-1078

Privacy in the workplace

Organizations must find ways to accommodate employees' personal technology use while also meeting regulatory and other requirements.



Parthiv Sheth
Khalid Wasti
A. Michael Smith

Illustration by Doug Ross

Digital technology has changed workplace behavior—and expectations—for both employees and their employers. The ubiquitous use of smartphones and other devices, company issued and personal, places communications and data management continually at users' fingertips. Internet use alters the traditional dimensions of employees' work flexibility requirements and need for expression, as well as employers' need to monitor employees' online activity.

Employee concerns have been amplified by the ever-evolving technologies and data collection methods that can seem personally intrusive. Any privacy expectations employees may have are being curtailed by privacy policies, privacy pop-up screens during computer log-ins, background checks, and other workplace measures. At the same time, governments worldwide have issued regulatory guidance to address privacy issues, but guidance often falls short when it comes to balancing employers' needs to

Evolving privacy expectations are changing where employees, and their employers, draw the line.

monitor and employees' expectations of privacy. Both noncompliance with regulations and balancing privacy needs represent major concerns.

Of respondents to PricewaterhouseCoopers's (PwC's) Global State of Information Security Survey 2016, 32 percent of security professionals say their board members review security and privacy risks—up from 25 percent in 2015. Employees remain one of the most-cited sources of compromise, with 34 percent of respondents citing current employees as sources of security incidents and 29 percent saying former employees were sources. Organizations have legitimate reasons for wanting to keep tabs on employee data, but employees also want some measure of protection from prying eyes. Evolving expectations on both sides are changing where employees, and their employers, draw the line. Internal auditors tasked with examining privacy in the organization should know where the risks lie, and what requirements their clients may face.

GLOBAL PRIVACY LAWS AND REGULATIONS

Organizations need to carefully consider the privacy-related legal requirements that apply to areas in which they do business. A subset of some of the main laws and regulations affecting privacy worldwide may be helpful for internal auditors looking to assess the potential risks.

EU-U.S. Privacy Shield was approved in July 2016–in the form of a data transfer framework between the U.S. and EU member states–to replace the defunct Safe Harbor agreement after intense negotiations between the U.S. Department of Commerce and the European Commission. At first blush, the Privacy Shield seems to resemble Safe Harbor, but closer inspection reveals that it introduces increased compliance complexities for U.S. businesses. The framework includes stricter requirements for enrolling and monitoring, additional third-party risk management considerations, new avenues for data-subject complaint escalation, and further limitations on government access to personal data. Employers must decide whether to participate in the new data transfer framework or use an alternative method to establish adequacy. More importantly, the decision about a data transfer method must be viewed in consideration of the General Data Protection Regulation–a much larger compliance obligation for U.S. companies that profile or collect data from EU citizens.

U.S. Securities and Exchange Commission's Regulation Fair Disclosure requires its issuers to disclose material information to the general public in a broad and nonexclusive manner. Registrants, therefore, must safeguard such information from inappropriate access and disclosure, in part through monitoring activities.

Japanese Act on the Protection of Personal Information defines personally identifiable information (PII) as any information about a living individual that could identify the individual by name, date of birth, or other description contained in such information. The act imposes data protection requirements on PII, including securing prior consents from individuals before exchanging or disclosing PII to third parties. The act was amended in September 2015 to require organizations that employ Japanese citizens to comply with the cross-border exchange requirements for PII before September 2017.

Australian Privacy Act and Australian Privacy Principles affect public and private entities in Australia as well as overseas businesses that manage the employee personal information of Australian citizens. The act and the principles specify requirements for active maintenance and notification of privacy policy and for extending liability, including the imposition of fines, to overseas businesses in cases

READ "Bashing the Boss Online" on InternalAuditor.org to learn about privacy issues surrounding employee use of social media.

DRIVERS OF PRIVACY DISRUPTIONS

Historically, employee monitoring has been limited to checking internet and email usage. Today, digital disruption trends powered by mobile devices, social media, analytics, big data, and the Internet of Things have opened up a host of additional channels for employee activity. Plus, increased competition has fueled mergers and acquisitions, as well as use of offshoring models and reliance on third parties, resulting in constantly changing privacy expectations in the workplace. Organizations are also starting to apply data analytics to better match people to jobs and to more efficiently and cost-effectively recruit, manage, and retain talent. Employees have a need to be heard and to contribute, and they use internal messaging boards and social media sites to do that. Most organizations do not even realize how much data is being collected and analyzed—and exposing them to legal and compliance risks.

Employee Expectations With the rise of a constantly mobile and fluid workforce and the consumerization of technology, trust is essential in the digital world. More and more employees expect to use their own devices and applications at work, as well as cloud services they're familiar with, because they believe those mechanisms make them more productive.

As employees use these devices with greater frequency, and as they become increasingly responsible for the data they hold in their cloud accounts, trust becomes a more significant factor. For instance, who's responsible if cloud data gets stolen or a device gets hacked? If disabling software is installed to protect the employer, what is that employer's responsibility for any personal information that gets lost? If the company comes under investigation by the authorities, would personal devices and data have to be handed over?

Employees might be more inclined to use wearable technology such as a smart watch if the information collected were leveraged for managing work hours or stress levels. They may trade personal data for flexible working hours, free health screening, and fitness incentives and approach data sharing more openly if the information is anonymized and shared at an aggregate level. Wearable technology, GPS tracking devices, radio frequency devices, and video cameras deployed in mobile workforces have great potential to track employee movement and productivity, but at the same time, each individual will have a personal limit to what is considered shareable.

Employer Expectations and Drivers Employers' concerns generally center on the need to protect themselves from loss of confidential information, shield against cyber threats, and comply with laws and regulations. Those needs require that employers monitor employee communications on company-issued computers, cell phones, tablets, and social media sites. Employers also need to collect personal information, such as Social Security numbers and health-related information, to provide health and compensation benefits. Companies are expected

of breaches that result in the loss of an Australian citizen's PII.

U.S. National Labor Relations Act protects the rights of employees to organize and bargain collectively with their employers and to engage in other protected concerted activity. Employers are prohibited from restricting employees from acting together, with or without union, to address work conditions that affect their personal lives. The provisions extend to conversations carried out in personal email accounts and social media sites.

General Data Protection Regulation (GDPR) for EU members was officially adopted by the European Commission in April 2016 and goes into effect in May 2018 after a two-year transition period. The GDPR strengthens European data protection laws, giving EU citizens greater say in how their digital information gets collected and managed. This complete overhaul of EU privacy confers regulatory authority over any business that offers products or services in the EU and over any business that tracks and stores EU citizen data, as well as the authority to fine violating companies up to 4 percent of their annual global revenues. New compliance requirements include an appointed privacy officer, privacy by design and default in products and services, the right to be forgotten, additional privacy impact assessments, and complete inventories of personal data and third-party data processors.

U.S. E-Government Act of 2002 requires that a federal agency conduct a "privacy impact assessment" before developing or procuring an IT system or a project that collects, maintains, or disseminates PII about members of the public. The act also sets forth uniform confidentiality protection requirements regarding such data.

to act reasonably regarding their possession of that personal information and to respect employees' rights to privacy. E-discovery tools are now more commonly deployed to investigate suspicious behavior, and so are data loss prevention tools to monitor network traffic and secure computers.

Regulatory Landscape Regulatory developments in recent years have focused mainly on the types of data that should be protected, such as personally identifiable information (PII), health information, financial information, and certain demographic information such as income and union representation. Employees in the U.S. have minimal expectations of privacy compared with their counterparts in Europe and Japan, where privacy expectations are absolute and supersede most other laws and regulations despite varying from country to country.

Employee rights are protected by privacy laws such as the Constitution's Fourth Amendment, the Electronic Communications Privacy Act, and the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and various European Union (EU) data protection laws in EU member states. However, outside of specific data privacy laws such as HIPAA, interpretations of those laws and regulations are based on reasonable expectations of privacy and refer to both an employee's expectation and an employer's implementation of privacy policies in the workplace. Certainly, *reasonable expectation* can be interpreted differently by different societies, and regulations as such have not kept pace with changing technological advancements. Each country has a multifaceted legal framework in place to govern that country's employers globally (see "Global Privacy Laws and Regulations" on pages 44-45 for examples).

TO COMMENT on this article, **EMAIL the author at parthiv.sheth@theiia.org**

> Organizations should take a holistic approach to managing privacy in the workplace.

AUDIT CONSIDERATIONS

Organizations should consider taking a holistic approach to managing privacy in the workplace. Moreover, their privacy framework should be agile enough to accommodate changing regulations. Internal auditors should evaluate the framework and other areas of privacy management to gauge the effectiveness of organizational efforts and overall governance.

Governance Framework Internal audit should evaluate the organization's governance framework, if one exists, to verify whether roles and responsibilities for managing privacy have been identified. An adequate framework will incorporate not only a chief information security officer or chief risk officer but also cross-functional partnerships across departments and geographies. Auditors should make sure that management defines a strategic vision and framework, if one does not exist, while ensuring it meets current and long-term business objectives.

Privacy Risk and Compliance Execution of a privacy risk and compliance assessment is an essential step in evaluating if the organization has translated its strategic vision and framework into practical implementation. This step entails a gap assessment of applicable laws and regulations within all geographies, as well as the discovery and data flow mapping of data elements that are stored, transmitted, or transferred either on organizational networks or on hard copies. Internal audit should execute such assessments periodically and

Approximately 70% of privacy professionals say complying with the General Data Protection Regulation will require additional budget, according to Baker & McKenzie's Preparing for New Privacy Regimes.

SOUND PRIVACY PROGRAM

An effective privacy strategy comprises numerous practices. Organizations that manage privacy well typically feature several components in their approach:

- An organizational view of what privacy means.
- An understanding of how privacy and data protection fit into the organization's overall business strategy.
- Complete knowledge of what data is held, where it is, and who has access to it.
- A clear understanding of data ownership and of circumstances under which data is protected and under which it is not.
- Understanding and management of the risks introduced to the data by third parties.
- Data governance that ensures data is being used for the purpose that the organization has committed to, and nothing more.
- A privacy model with agility in mind, given the ever-changing privacy landscape.
- Thorough familiarity with legal obligations in the U.S. and abroad, and tracking of developments in regulatory enforcement actions and case law.

perform a risk assessment on a more frequent basis to evaluate the impact of organizational and regulatory changes.

Policies, Processes, and Controls Auditors should be proactive in guiding management to develop new—or enhance existing—policies, processes, and controls by incorporating privacy-by-design (i.e., embedding privacy into the design specifications of technologies, business practices, and physical infrastructures). They should, for example, evaluate the privacy impacts of new products, third parties, mergers and acquisitions, systems, and technologies; and when the organization enters new markets, auditors should make sure controls are in place to manage privacy requirements. Controls around investigations of employee behavior on an organization's networks and computer systems should be in place and evaluated by auditors periodically. These controls might include using e-discovery tools aimed at validating internal approvals, clearly articulating the purposes for monitoring that are proportionate to the investigation underway, and involving lawyers when necessary.

Training and Awareness When policies set the tone of data protection management and guidance, employees and third parties should be trained in their roles and responsibilities. Training and awareness should be adaptive to meet specific needs at every level: executives, management personnel, human resources personnel, supervisors, IT staff, and so on. Auditors can advise management on the development of such programs and then periodically assess employee participation to gauge training compliance.

Monitoring and Response Monitoring the environment to ensure compliance with privacy regulations is not just about deploying e-discovery and other tools over the network. It requires ongoing communication and periodic reporting across departments and geographies to help identify and isolate privacy concerns timely. However, organizations with over-the-top monitoring practices could encounter incidents or privacy crises with no warnings, resulting in their reacting reflexively. In their haste, decision makers could fail to consider who should be in the room making decisions, how emerging issues should be prioritized, and how to think strategically beyond the next 24 hours. Internal auditors should ensure that the business has incident management and response capabilities that align with best practices and overall business objectives.

A MATTER OF TRUST

Trust in the digital age can be difficult for employers to navigate because it's closely intertwined with risk, security, and privacy. Nothing is hidden in the digital world; the views and opinions of former and current employees are available for everyone to see, and employees expect a clear explanation of what they are contributing and how they're to be rewarded for it. For these reasons, ongoing trust levels must be built between employers and employees by way of transparency in their day-to-day interactions, and a mutual interest in balancing both parties' priorities. ia

PARTHIV SHETH *is a director in PwC's Risk Assurance practice in New York.*
KHALID WASTI, CIA, CPA, CISA, CITP, *is a partner in PwC's Internal Technology Audit Solutions practice in New York.*
A. MICHAEL SMITH, CPA, CISA, CISSP, *is a national partner in PwC's Internal Technology Audit Solutions practice in the U.S.*

A Unified Approach to Compliance

Businesses benefit from a proactive partnership between internal audit and the compliance function.

Jane Seago

In today's world, virtually every organization is subject to some sort of regulation. Consequently, virtually every organization has some structure in place to ensure ongoing compliance with those regulations. And for good reason: Failure to comply can result in financial penalties, possible jail time for executives, and significant reputational damage.

In small organizations, the compliance function may consist of just one person—perhaps handling compliance on the side. Large organizations are more likely to have a full-fledged compliance function, often set up as a compliance and ethics department, usually under the legal umbrella. In very large organizations, the compliance and ethics programs may be separated because of the workload required of each.

But regardless of the company structure, any organization that is not coordinating its internal audit and compliance functions is missing a beat. "When internal audit ensures the compliance program has a strong structure, the compliance department can ensure the business has a strong program that mitigates business risk," says Cecelia Jefferson, an attorney and compliance professional in Amelia Island, Fla. A former director of alcohol, tobacco, and firearm compliance for Walmart U.S., Jefferson skimps no words in describing the critical role internal audit plays in compliance. "Once the compliance department understands the year's business goals, it will design any changes or upgrades needed to ensure the business remains compliant. Internal audit should be included in these discussions."

Understanding the business objectives, and how the compliance department plans to assist the business in achieving them, helps internal audit determine where, how, and how often to provide support. Identifying those questions is relatively straightforward. Answering them in the most effective way, especially in the face of competing demands on resources, can be tricky.

INTERNAL AUDIT AND THE COMPLIANCE FUNCTION

There are probably as many ways for internal audit to perform its role in compliance as there are internal audit and compliance functions worldwide. One approach is for internal audit to engage with compliance on two levels, which

"Internal audit needs to discover how the compliance function is getting its information."

Nancy Haig

"One of the key objectives of internal audit as articulated in our charter is to 'assist the directors to discharge their duties in ensuring that the relevant compliance and risk management processes are in place.'"

Jenitha John

Nancy Haig, director of internal audit and compliance at a global consulting firm headquartered in New York, calls "macro" and "micro." At the macro level, internal audit examines the effectiveness of the organization's compliance program. "Internal audit needs to discover how the compliance function is getting its information," Haig explains. "Is it doing regular scans of the environment? Is it getting qualitative and quantitative input across the board? Is it calculating the residual risk in all compliance areas?"

At the micro level, internal audit drills down on selected risks the compliance function has identified as priorities. If the compliance function has done a risk assessment, it may be possible to leverage it; if not, internal audit may need to perform one. Mitigation plans are only as good as the risk assessment on which they are built.

Naohiro Mouri, executive corporate officer and chief internal auditor at AIG Japan Holdings in Tokyo, also takes a two-pronged approach. "We audit compliance in itself, as a separate audit engagement, but we also look at compliance risk that is embedded in the processes of the business units as we do our regular audits of them."

The internal audit charter is critical in defining internal audit's role in compliance. "One of the key objectives of internal audit as articulated in our charter is to 'assist the directors to discharge their duties in ensuring that the relevant compliance and risk management processes are in place,'" notes Jenitha John, CAE at FirstRand Bank in Johannesburg, South Africa. In her bank, the internal audit function performs compliance audits to assess whether there are adequate and effective controls in place for the organization to comply with relevant legislation and to ensure ethical business conduct. Internal audit follows up on control gaps by monitoring remediation, identifying thematic compliance issues across the organization, helping guide the compliance function to focus on high-risk areas, and assessing and providing an opinion on the maturity of the organization's regulatory risk management process. These efforts are paying off, says John, who reports "a downward trend in significant compliance audit findings."

Debbie Shelton, director of IT security and compliance at LG&E and KU Energy LLC in Louisville, Ky., offers a slightly different approach to the types of engagement between internal audit and compliance. "With a detailed understanding of the organization's compliance risk assessment, internal audit can first focus on the foundations of the assessment," she explains. This leaves responsibility for the assessment where it belongs—in the business—with internal audit adding assurance that the assessment methodology is sound or raising questions about levels of residual risk that appear to be in excess of the approved risk appetite. She further notes that internal audit should be delving into the assumptions that are made and documented within the assessment model, how the assumptions are communicated, and whether all those inputting into the model understand the assumptions in the same way.

At the second level of Shelton's approach, which occurs once the foundation has been determined to be sound, internal audit can focus on the actual entries by examining issues such as how the organization ensures completeness, whether a requirement-by-requirement accountability document is provided to all those involved in the assessment, and how those with accountability ensure updates are made timely.

Approaches differ by company, but all are aimed at securing positive outcomes. Greg Jordan, senior vice president and CAE at Nationwide Insurance in Columbus, Ohio, describes a tangible

81% of 150 compliance officers agree that compliance will need to optimize operations to manage more complex risks with tighter resources, according to Accenture's 2016 Compliance Risk Study.

BASICS OF AUDITING COMPLIANCE

The following terms and concepts are sure to play into internal audit's compliance activities:

- Inherent risk – The risk level or exposure without considering the actions that management has taken or might take (e.g., implementing controls); often falls into one or more of four categories: legal, financial, business, and reputational.
- Residual risk – The remaining risk after management has implemented a risk response.
- Compliance risk – The threat posed to an organization's financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice. Shelton defines compliance risk in broad categories: assessment risk, access risk, people risk, response/recovery risk, evidence suitability and retention risk, and change management and segregation of duties risk. Specific examples of compliance risk include worker safety regulations for manufacturers; amount of margin allowed for investment accounts; managing crisis and remediation while defending the organization and its executives/board members against legal enforcement; levels of commission to sales agents; and banking legislation relating to customer identification and verification, financial advice, and lending.
- Pertinent standards – According to Haig, her "go-to standards" when dealing with compliance are IIA Standard 2110: Governance and Standard 2120: Risk Management. Also see Standard 2050: Coordination.

benefit of the expanded role internal audit plays in compliance in his company: Internal audit staff is rotating out of internal audit into the compliance department, and compliance professionals are moving into internal audit. "Roll the clock back a few years," he says. "That sort of career path didn't exist."

BUILDING A PARTNERSHIP

Working together effectively requires a strong commitment to collaboration and partnership. Both internal audit and compliance must share a focus on best practices, cooperative effort, and information sharing.

Mouri's internal audit team relies on the compliance department to provide education on changes in regulations that might generate new risks or reporting requirements. For their part, when internal auditors find issues in their audits that indicate a regulatory breach, and if that breach is significant enough, they ask the compliance function to report it to the regulators. "They are the experts in this area," he explains. "We rely on their judgment rather than making compliance decisions ourselves and reporting to the regulators."

Jordan notes a similar activity within Nationwide. "We have a regulatory assessment distribution process we audit regularly," he says. "It monitors regulatory activity that affects our business units, what changes these regulatory activities entail, what dates the changes become applicable, and which business units are affected and need to receive information to incorporate into their business plans. Compliance tracks the

"We rely on [the compliance department's] judgment rather than making compliance decisions ourselves and reporting to the regulators."

Naohiro Mouri

"Speak with subject matter experts in the company. Seek documentation outlining why key compliance decisions were made."

Debbie Shelton

"Internal auditors served as a second set of eyes to ensure we were appropriately identifying and mitigating all risks and the proposed solutions did not create problems for the program or stakeholders."

Cecelia Jefferson

"We talk with general counsel and compliance during regular audit planning for each engagement, to make sure nothing of a regulatory nature has changed that would affect the audit."

Greg Jordan

regulations and internal audit understands the key compliance-related risks."

Shelton proposes that collaboration center on identifying all compliance requirements and reviewing an existing risk assessment of requirements or collectively completing one. She further suggests, "Use the authority each organization has in engaging participants in the audit. Speak with subject matter experts in the company. Seek documentation outlining why key compliance decisions were made."

Collaboration may best be accomplished by simply talking to each other. Haig describes an effective monthly meeting at one of her previous employers, in which the CEO and the heads of internal audit, compliance, and legal discussed emerging risks, trends, and mitigation plans. Similarly, in her prior role at Walmart, Jefferson led a consortium of business stakeholders, including compliance and internal audit, which met on a weekly basis to discuss activity within the compliance program. The internal auditors, Jefferson says, "served as a second set of eyes to ensure we were appropriately identifying and mitigating all risks and the proposed solutions did not create problems for the program or other stakeholders."

Jordan conducts his own frequent meetings with his counterparts—the chief compliance officer and the chief risk officer—and engages in a monthly meeting between internal audit and the compliance department in which they review any changes in the organization's risk landscape and inform each other of pertinent upcoming activities. "We talk with general counsel and compliance during regular audit planning for each engagement, to make sure nothing of a regulatory nature has changed that would affect the audit," he adds. "We also invite compliance to our internal audit status meetings and, when there is an issue of regulatory impact, to closing conferences with audit clients."

It's not all a matter of meetings, however; technology plays a role in facilitating collaboration, as well. John notes the need for formal combined assurance platforms that drive ongoing and consistent engagement between internal audit and compliance. One of the key levers to drive this collaboration is eGRC technology, which improves visibility of the organization's compliance risk profile. John's organization is currently implementing an eGRC platform across governance functions, including compliance, to drive holistic compliance risk management.

LEVERAGING THE COMPLIANCE RISK ASSESSMENT

One of the most common areas of cooperation and coordination between internal audit and compliance focuses on internal audit's use of the compliance risk assessment done by the compliance department, as either stand-alone output or as a contribution to the organization's enterprise risk assessment. Given that most organizations operate under time and resource constraints, getting multiple uses out of a single work product is advantageous. But, due diligence must be done. In this context, that means before relying on the compliance department's compliance risk assessment, internal audit must review that risk assessment for effectiveness and to ensure that the compliance function has done, in Haig's words, "an effective job."

Assessing the risk assessment's effectiveness starts with asking pertinent questions about the frequency of update, the sources of the information, the extent of coverage of regulatory risks, the amount of engagement with and involvement of the legal department, the prioritization of risks based on the residual risk assessment, the evaluation of controls to manage and mitigate specific risks, the alignment

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

ELEMENTS OF A COMPLIANCE PROGRAM

Compliance program elements may include:

- Policies and procedures.
- Narratives and control documentation.
- Risk, responsibility, and compliance matrixes.
- Metrics, such as degree of employee knowledge/awareness of compliance risks and benchmarks of peer organizations.
- A framework that lays out the organization's compliance risk landscape and organizes it into risk domains, and a methodology that contemplates both objective and subjective ways to assess those risks.
- Root cause analysis process.
- Communication plans for internal and external audiences.
- Training plans focused on key compliance risk areas.
- Testing plans.
- Monitoring processes.
- Consistent enforcement, plus escalation and response plans in the event of violations.

between the results and the organizational risk appetite, and the degree to which irregular findings are investigated and controls added as needed. In addition, it may be useful to consider whether someone outside the compliance department can pick up the department's workpapers and see how the compliance staff came to its conclusions relative to frequency and magnitude of risk.

Shelton proposes another test that would be well-suited for organizations in which several groups or departments have processes for compliance assessments. "Internal audit can assess whether consolidating best practices into an organizational program might be of benefit and, if so, make—and possibly facilitate—that recommendation."

John explains that her company's assessment of the effectiveness of compliance risk assessments is based on a regulatory risk management maturity model. Specifically, she notes certain elements she calls fundamental to compliance risk assessment effectiveness:

- The governance and strategy in place to drive the consistent and complete assessment of compliance risk in the organization. She elaborates, "This includes an evaluation of governance committees, frameworks, senior management (risk owners) sign-off on the regulatory universe/risk assessment, and consideration of the involvement and influence of the compliance function in the industry's regulatory landscape."
- The adequacy and effectiveness of the compliance risk resources, including the level of skills within the compliance function.
- Identification, measurement, and risk mitigation for high-risk legislation as per the regulatory universe. This includes assessing whether sufficient key risk indicators have been formulated to monitor risks and continually strengthening the compliance control environment.
- Risk monitoring plans to make sure that first and second lines of defense ensure the adequacy and effectiveness of controls in place to mitigate risks identified.
- Risk reporting processes to ensure that a clear and complete risk profile of the organization is reported and monitored appropriately.

TRUE PARTNERS

Regardless of how engagement between internal audit and compliance occurs, there is broad support for ensuring that this engagement does happen. Internal audit can actively drive combined assurance in the organization by collaborating with the compliance and risk management functions in performing audits. This collaboration improves the coverage of compliance risk assurance and reduces duplication of effort.

And, ultimately, internal audit has an innate need to become involved in assessing compliance. According to The IIA's International Professional Practices Framework, the mission of internal audit is to "enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." In other words, understanding, evaluating, and mitigating risk are internal audit's purpose. For many organizations, there are few, if any, risks more significant—in financial and reputational terms—than failure to comply with existing regulations. Internal audit cannot fully achieve its mission if it does not include compliance in its remit.

"In my company, compliance and internal audit are true partners in risk management," Jordan says. "Our viewpoint is that it's better for everyone if we can work together to reduce our regulatory burden. We focus on achieving the benefits for the business and doing the right things by the stakeholders."

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

Understanding the powers of persuasion and applying key rhetorical skills can improve the work of any internal auditor.

Murray D. Wolfe

Internal auditors are fortunate to have robust professional standards to help guide and inform the performance of their work. One of the main pillars of these standards, of course, is the need to remain independent from the organization so that audits can be conducted without bias. Independence helps better position auditors to identify solutions to key problems, and it prevents them from taking direct action to implement those solutions.

Within the ambit of their professional requirements, practitioners can only persuade others to act. And while persuasion may not be a formal requirement for auditors, the ability to persuade is key to the success of their work. Even a beginning auditor quickly realizes that presenting evidence collected during fieldwork merely as a succession of facts often doesn't convince clients to take action. To capture stakeholders' attention, and elicit a response, auditors need to possess a degree of rhetorical skill.

Although rhetoric is a complex subject that can take years of study to master, the basic principles are relatively easy to grasp. Understanding these principles and applying them to the practice of internal auditing can help internal auditors get their messages heard—and acted upon.

THE TRIVIUM

Rhetoric refers to the use of language to persuade and instruct. Through the Middle Ages, European universities taught rhetoric to beginning students as one of three foundational topics known as the trivium. Logic and grammar, the other two foundational topics, refer to the mechanics of thought and analysis, and the mechanics of language, respectively.

Internal auditors essentially follow the trivium in their work. After gathering evidence through fieldwork, they apply logic to analyze evidence and identify problems and solutions. They also use grammatical rules to structure text within reports and memoranda.

the POWER of *rhetoric*

Applying the trivium requires a balanced approach—too much focus on the mechanics can lead to ineffective communication. Internal auditors need to consider all three trivium components evenly and avoid the common trap of collecting too much evidence or performing too much analysis in the belief that it will help strengthen their reports.

Although most individuals learn grammar early in life and are taught to analyze evidence in college, seldom do students receive direct education on rhetoric—except perhaps through an undergraduate class in English or philosophy. Even then, instruction typically lacks specific focus on business writing or internal audit reports. Moreover, a large portion of internal auditors are accountants trained to focus on numbers-based financial information. Yet in practice, most auditors are required to devote a great deal of time and effort to work that demands skillful application of the written word. For this reason, many practitioners can benefit from additional guidance on how to apply key principles of rhetoric to their work.

ARISTOTLE'S TRIANGLE

The Greek philosopher Aristotle, considered the "father of rhetoric" by many scholars, defined three key components of rhetoric—the speech

PHOTO: PANOS KARAS / SHUTTERSTOCK

itself (text), the speaker delivering the speech (author), and those who listen to the speech (audience). Collectively, these components form the Rhetorical Triangle. For internal auditors, the triangle's three points equate to the report or memoranda, the engagement lead, and clients or stakeholders.

All three of the rhetorical triangle components are interrelated, and they are essential to the success of internal audit consulting or assurance work. Each should be considered before any engagement and kept in mind throughout the engagement life cycle—especially during the reporting process.

The Author Although the engagement lead would be considered the primary author, each of the engagement team members plays a supporting role by authoring observations and recommendations that are then compiled into an integrated report. The draft reviewer also has a role to play, ensuring that the final report meets the internal audit function's standards and fulfills the purpose defined in the planning document. "Authors Within an Engagement," on page 58, summarizes the typical authors, using an accounts payable audit as an example.

> **The need to consider ethos begins long before the start of the engagement.**

The Audience The intended audience should be considered with each engagement. Audience members are not homogeneous—each will have different perspectives and expectations. For this reason, internal auditors need to consult with them and consider their perspectives before the engagement begins. Using the "Responsibility Assignments for the Engagement Audience" matrix (page 59), based on an accounts payable audit example, can help identify key audience members.

The Written Text Once engagement fieldwork has been completed, the authors compose a written report containing the results of the audit work. The report represents perhaps the most important communication from the audit process, and the best chance to get management's attention.

THREE TYPES OF APPEALS

When crafting the audit report, three separate but interrelated "rhetorical appeals," originally defined by Aristotle, need to be considered and applied: ethos, logos, and pathos.

Ethos is an appeal to the audience's perception of the honesty, authority, and expertise of the author. Closely related to reputation, ethos is established when the audience determines that the author is qualified, trustworthy, and believable. Because the term *ethics* derives from ethos, adhering to The IIA's Code of Ethics supports this appeal.

Speaker and business consultant Harry Beckwith's book, *Unthinking: The Surprising Forces Behind What We Buy*, discusses how key marketing principles linked to the drivers of human behavior fit within a general rhetorical framework. Several questions adapted from the book's "Unthinking Marketer's Checklist" can help internal auditors determine how well they fulfill the ethos appeal:

- What assumptions does your audience likely make about you and internal audit, what you produce, and the level of service or advice you provide?
- Is there a way to take advantage of their positive assumptions? What can you do to overcome their negative assumptions?
- Do you create the expectation that what you produce and the level of service or advice you provide will be exceptional?
- Are you using all available marketing channels to create an impression of excellence?
- Are you managing all your processes to ensure that you regularly meet, and sometimes exceed, expectations?

The need to consider ethos begins long before the start of the engagement. Ethos is supported by the structure and governance of the internal audit function as well as by the selection of team members—including alignment between the type of engagements to be performed and the team's qualifications, education, and training. Ethos appeal is also established by choosing to comply with audit standards and other professional requirements to demonstrate a high level of credibility, build trust, and gain a favorable reputation.

Logos appeals to the audience's sense of logic, encompassing factors such as the reason and analysis used, the underlying meaning communicated, and the supporting facts and figures presented. The written document's visual appeal—diagrams, charts, and other elements—as well as how the information is organized, presented, and structured, also factor into logos.

In his book, Beckwith notes the importance of story to convey meaning, and how from the time we're born we learn about the world around us through narratives. This aspect of logos continues to be important throughout

21% of stakeholders say that internal audit does not communicate which organizational risks/activities aren't covered by the audit plan, according to The IIA's Six Audit Committee Imperatives report.

AMPLIFYING APPEALS: ACCOUNTS PAYABLE AUDIT

Putting the appeals into practice requires a focused, concerted effort. Using a hypothetical accounts payable audit, the examples below demonstrate use of the rhetorical appeals as well as the engagement team's roles and responsibilities.

Enhancing Ethos Ensure the engagement lead has undergone training specific to accounts payable, preferably as a designated accountant, and also possesses experience either working within the accounts payable department or auditing the area as a practicing internal auditor (or even as part of an external audit of the financial statements). The entire engagement team needs to be sufficiently qualified—as demonstrated through a combination of education, certifications, and experience. Moreover, each team member should be listed in the planning document, along with his or her qualifications, and introduced during the opening meeting. When team members possess an internal audit-specific designation, it implies they are required to comply with a clearly defined code of professional ethics, thereby contributing to the ethos appeal.

Maximizing Logos As part of the planning process, internal auditors should perform adequate research before starting accounts payable fieldwork. Research can include the review of internal information (e.g., previous accounts payable reports; recent examples of issues related to accounts payable), as well as external benchmarking information and practical models and frameworks relevant to accounts payable.

The engagement plan and approach should align with the scope and purpose of the accounts payable audit, as described in the planning document. The audit report should convey a strong impression of thoroughness and appropriate follow-through, supported by an adequate understanding of the function and its relationship to business operations. The report should be written following a standard template, defined protocols (including a style guide), and examples of past audit reports.

From a structural perspective, the audit report should be reviewed and edited by the CAE, and perhaps other audit team members, to minimize errors before issuance. The review should ensure that observations are adequately supported by relevant evidence, recommendations are practicable, and the information presented is both clear and concise. In addition, the process should include a checklist of review items such as data accuracy within tables, consistent use of terms, definition and consistent use of acronyms, correct spelling and grammar, consistent use of fonts, and correct titles and spelling of names.

Optimizing Pathos Auditors should devote adequate attention to key accounts payable staff during fieldwork to understand and acknowledge the pressures they face daily, as well as the effect of any recent changes or emerging areas of risk. Accounts payable is a "downstream" function that serves as the last bastion of control before cash leaves an organization, and it is often blamed for the consequences of actions by "upstream" employees or functions. Auditors should keep this potential for finger-pointing in mind throughout the engagement and consider the effect it may have on accounts payable employees. Moreover, recognizing the good work done by accounts payable staff to catch and correct invoice errors before paying vendors, as well acknowledging any information internal audit obtains through accounts payable for identifying upstream risk areas, can help establish an effective relationship.

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

our lives. Beckwith also points out that we “experience the world through our senses, particularly our eyes.” He emphasizes that design and visual attractiveness are key to engaging an audience comprising “visual animals.”

Beckwith uses several questions to assess the design and presentation of material. Two of these questions, which focus on simplicity, may be useful for internal auditors:

- » Is what you are presenting easy to understand?
- » Is your design simple and beautiful?

Auditors’ need for logos is addressed by their written report’s executive summary, detailed observations, and recommendations, as well as appendices with secondary information that can be used to further instruct the audience. The report describes the drivers and overall purpose of the engagement, findings, and proposed solutions. Ultimately, from a rhetorical standpoint, auditors try to tell a convincing, self-contained short story that conveys key messages to the audience. The structure and format of the report, together with its textual content and visual elements, also support the logos appeal.

Like ethos, the logos appeal is fulfilled long before an individual engagement begins. It starts with the rational, periodic assessment and identification of high-risk areas requiring internal audit’s attention, resulting in development of the strategic and annual audit plans. Auditors then undertake engagements, executing steps to collect valid and relevant evidence to justify conclusions and make meaningful recommendations.

Pathos focuses on the audience’s irrational modes of response.

Pathos is an appeal to the audience’s emotions, either positive (joy, excitement, hopefulness) or negative (anger, sadness). It is used to establish compassion or empathy. Unlike logos, pathos focuses on the audience’s irrational modes of response.

Aristotle maintained that pathos was the strongest and most reliable form of persuasion. Pathos can be especially powerful when it is used well and connects with the audience’s underlying values and perspective. Used incorrectly, however, pathos can distort or detract from the impact of factual evidence.

AUTHORS WITHIN AN ENGAGEMENT

ROLE	RESPONSIBILITY	EXAMPLE: ACCOUNTS PAYABLE AUDIT
PRIMARY	Draft and distribute the planning documents as well as the engagement report, based on support provided by the engagement team.	Engagement Lead: » Senior Auditor
SECONDARY	Execute assigned portions according to the engagement plan, identifying observations and drafting recommendations.	Engagement Team: » Auditors » Technical Experts
REVIEWER	Ensure that expectations within the planning document are fulfilled and discussed within the report.	CAE

Use of dynamic visualization tools for internal audit communication is expected to increase from 7 percent to 35 percent in the next 3 to 5 years, according to Deloitte's Evolution or Irrelevance study.

RESPONSIBILITY ASSIGNMENTS FOR THE ENGAGEMENT AUDIENCE

COMPONENT	ROLE	EXAMPLE: ACCOUNTS PAYABLE AUDIT
RESPONSIBLE	Leader in charge of the primary area being audited, usually at the vice president or director level.	Corporate Controller Director, Accounts Payable
ACCOUNTABLE	Executive team member, responsible for the area at the highest level of management.	Chief Financial Officer
CONSULTED	Leaders in charge of areas dependent on or affected by the area being audited, but secondary to it, at the vice president, director, and manager levels.	Supply Chain Management Operations Management
INFORMED	Interested in the results of the engagement, but not directly concerned with the area being audited except at the highest level.	Executive Team Audit Committee External Auditors

Several questions adapted from Beckwith's guidance can be used to evaluate how well a message appeals to pathos:

- Does your message appeal strongly to emotions, or is it merely rational?
- Have you identified the emotional forces that drive people to accept your observations and recommendations and those that might drive them away?
- Is your message presented optimistically? Is it adequately focused on achieving good outcomes and balanced with avoiding bad ones?
- Is your report story-based? Are you telling the story well? Is it authentic and honest? Will it resonate emotionally with your audience?

Auditors should "walk a mile in someone else's shoes" and look for ways to better understand the audience's perspective. Attention to pathos can help support not only audit objectives, but the overarching goal of creating a "win-win" solution. Auditors should also be mindful of their overall tone and word selection, and ensure they balance negative and positive comments—giving credit where credit is due.

To some extent, pathos is interdependent on ethos and logos: Negative results can be reduced somewhat by the positive effect of the other two appeals. For example, audience members are more likely to accept bad news from someone they trust and respect, and who they know has followed a rational, structured approach to the engagement. But at the same time, ethos and logos can be offset by negative pathos. Distributing audit results before stakeholders have had a chance to review them, for instance, could potentially be detrimental to internal audit's reputation and trustworthiness. Preferred practice generally consists of holding regular meetings with stakeholders over the course of the engagement, maintaining transparency, and providing stakeholders an opportunity to refute audit findings or provide evidence that counters internal audit's observations.

HUMAN NATURE

All three elements of rhetorical appeals play an important role in communication. And while none should be neglected, auditors should pay particular attention to pathos. As Beckwith observes, "During our decision making, the organ that processes our data sits on the sidelines while our feelings do the work. When our feelings reach their decision, they summon our brains to come in and draft the rationale, a task it does so well that it manages to convince us that it's right—and that it was in charge the whole time."

The dominance of feelings over reason is part of human nature, and internal auditors should consider this when planning and executing engagements and reporting the results. By doing so, auditors can help ensure audiences accept their message and make recommended improvements, ultimately promoting the function's success and that of the clients it serves.

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

The red flags

Internal auditors' knowledge of the business makes them ideal candidates to detect unethical behaviors.

Norbert Tschakert
Belverd Needles Jr.
Mark Holtzblatt

In its 2016 Report to the Nations on Occupational Fraud and Abuse, the Association of Certified Fraud Examiners (ACFE) estimates that organizations lose 5 percent of revenues in any given year to fraud, resulting in an estimated fraud loss of US$3.7 trillion worldwide. It is important to realize that fraud directly affects a company's bottom line. For instance, a US$100,000 fraud case in a company with a 10 percent profit margin would require an additional US$1 million in revenues to make up for the loss.

The longer a fraud goes on, the greater the financial damage to the organization. The findings from the ACFE report also indicate that the median loss and median duration of fraud schemes are lower when they're uncovered through active detection methods, such as surveillance and monitoring and active management review, than when detected via passive methods, like accidental discovery or confession. By improving their ability to recognize fraud red flags, internal auditors can better safeguard company

PHOTO: LJUPCO SMOKOVSKI / SHUTTERSTOCK

# of FRAUD

assets, reduce inefficiencies and litigation risk, and aid in satisfying increasing regulatory scrutiny.

RISK FACTORS AND FRAUD TYPES

Internal auditors should consider a red flags analysis customized to the risks and circumstances of their organization. Red flags do not necessarily indicate a fraud is taking place—they constitute warning signs that it could occur.

Red flags exist for many types of fraud, illegal acts, corruption, and other circumstances harmful to the organization, but employee or financial statement red flags are common in most types of frauds.

Financial Statement Fraud This type of fraud may involve misstating or omitting amounts or disclosures in financial statements. Financial statement fraud has been connected to restatements of financial figures; disclosure of internal control deficiencies; U.S. Securities and Exchange Commission Accounting and Auditing Enforcement Releases; auditor and law office changes; significant litigation, especially with stakeholders; related-party transactions; rapid turnover of key employees; a complex business structure; problems with regulatory agencies; declining sales and profits; loss of market share; and insufficient liquidity.

The primary motivation for financial statement fraud is personal enrichment through stock-based or performance-based compensation. This can include attempts to avoid adverse events, such as missing Wall Street expectations or violating covenant agreements. More altruistic considerations also exist (saving the company from bankruptcy and employees from unemployment), but are less common.

Employee fraud is the most common type of fraud, but it exhibits the smallest damage amount per case.

The internal audit function can analyze financial statements to uncover red flags related to financial statement fraud through procedures such as:

- Examining the relationship of present-year account balances with nonfinancial information (e.g., inventory vs. warehouse capacity or production vs. production capacity).
- Comparative analysis of account balances from the current year to balances of prior years and to expected results from the firm's forecasts and budgets.
- Assessment of the relative amounts of this year's account balances to other present-year balances to ascertain whether they conform to patterns of predictability based on the firm's history.
- A comparative analysis of account balances and ratios to industry benchmarks.
- Scanning for unusual or unexpected balances or transactions in account balances, listings of transactions, and journals, or any last-minute, senior-level management journal entries.

Inappropriate revenue recognition represents a significant percentage of financial statement fraud. By using analytical procedures, unexpected relationships among revenue, costs of goods sold, accounts receivable, cash flow from operations, and industry and competitor information can be brought to light for further investigation. Extensible business reporting language increasingly facilitates some of these tasks, enabling automatic ratio and trend analysis, or benchmarking against competitors.

Behavioral red flags linked to management fraud include inconsistent, evasive, vague, or implausible responses to internal auditor inquiries. To then direct the same questions to different levels of employees may bring such fraud to light.

Employee Fraud This fraud is committed against the organization for which the perpetrator works. While it is the most frequent type of fraud, it exhibits the smallest damage amount per case. Some examples include:

- **Employee theft of cash** in the form of unrecorded sales can be indicated by gaps in prenumbered documents (invoices), lower than expected revenue in a particular location, lower-than-expected revenue when a particular employee is working, and differences between customer and company records. Warning signs relating to employee theft of noncash assets include inventory shortage, missing work tools, altered documentation such as shipping documents, and unsupported journal entries to inventory or asset accounts.

- **Employee expense reimbursement fraud** warning signs include expenses exceeding budget or historical amounts, multiple receipts from the same vendor, travel expenses not being reviewed, and expense reports with no detail.
- **Payroll fraud** may be indicated by inadequate segregation of duties, a higher number of employees paid than employees actually working, former employees still on payroll, invented or real "ghost employees" on payroll, or inadequate supervision of employee work time.
- **Kickback scheme** red flags include increasing prices, larger-than-normal order quantities, decreasing quality, increased purchases from a favored vendor while decreasing purchases from other vendors, use of an unapproved vendor, complaints from unsuccessful vendors, and quality complaints from customers.

Additional areas of concern for employee fraud include misuse of corporate assets, conflicts of interest, fraudulent disbursements, bribery, economic extortion, and illegal gratuities. Lifestyle symptoms, as well as tips and complaints, are among the best indicators of these types of frauds (see "Behavioral Red Flags" on this page).

The ACFE also identifies common fraud perpetrator characteristics. Most perpetrators wait to learn about the company's internal control, so significant fraud activity only starts after about a year of tenure with the organization. The likelihood of fraud is highest when the perpetrator is under the greatest amount of stress (e.g., paying their mortgage or tuition for their children) and has increased authority in the organization. The perpetrator's level of authority is correlated to the size of the fraud, and males instigate more significant fraud cases than females.

BEHAVIORAL RED FLAGS

What makes a person decide to commit fraud? Criminologist Donald Cressey's fraud triangle theory outlines three contributing factors—perceived pressure, perceived opportunity, and rationalization. When an individual is feeling pressure, sees an opportunity, and can rationalize his or her actions, fraud is more likely to occur. The fraud triangle describes the "accidental" fraudster who is led to unethical conduct more through circumstances than existing intent. For the "predator" fraudster, often associated with antisocial personality disorders, opportunity alone may be enough to consider engaging in fraud.

In its 2016 Report to the Nations on Occupational Fraud and Abuse, the Association of Certified Fraud Examiners identified behavioral red flags that many fraud perpetrators exhibit:

- Living beyond one's means.
- Financial difficulties.
- An unusually close association with a vendor or customer.
- Control issues or an unwillingness to share duties.
- Wheeler-dealer attitude involving shrewd or unscrupulous behavior.
- Irritability, suspiciousness, and defensiveness.
- Addiction problems.
- Refusal to take vacations.
- Complaining about their lack of authority.
- Excessive gambling.
- Increased smoking.
- Making up excuses for missing documentation or shortages and finding scapegoats.

Most offenders are under increased stress, as they fear detection. This stress triggers changes in behavior, so the red flag is the change rather than a particular behavior. Besides personal enrichment, a negative work environment and employee dissatisfaction are common reasons for employee fraud as employees attempt to "get back" at their employers.

TECHNOLOGY AND ANTI-FRAUD TRAINING

Business knowledge frequently is a prerequisite for identifying red flags. Risks are often unique to the organization, and techniques to identify them include brainstorming, flowcharting, questionnaires, continuous monitoring, and data analysis.

Red flags help narrow the scope of information that internal auditors must review manually. For instance, not every processed payment can be reviewed each month. Data analytics can help identify payments that do

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

Trust Your Quality
to the Experts

Median losses are **twice as much** for victim organizations that lack **anti-fraud** controls, according to the ACFE's 2016 Report to the Nations on Occupational Fraud and Abuse.

not adhere to the expected flow and enable an internal auditor to deal with a much more manageable data set for further review.

Analyzing red flags applicable to the organization and incorporating them into the accounting information system (AIS) for continuous monitoring to set off automatic alerts has vast potential for many organizations, including small- to medium-sized organizations that are disproportionately affected by fraud. AIS log files can be used to identify which employee has made what changes at what point in time.

Anti-fraud training also teaches employees to recognize red flags, reinforces company policies, and explains steps that should be taken once red flags are identified. The result is an improved control environment, earlier detection of fraud, and deterrence of future fraud. Anti-fraud training can allow a company to progress from passive to proactive and organized when looking for red flags. Often, lower-level employees do not share knowledge about questionable transactions without being encouraged through such training.

THE IMPORTANCE OF EARLY DETECTION

Fraud investigators often state that there are no small frauds, only frauds that are caught early as perpetrators rarely stop and will continue to exploit a successful scheme. As recoverability is often difficult, prevention and early detection are critical to prevent frauds from growing and to avoid time-intensive, disruptive, and expensive investigations that could lead to reputational damage. Because of their knowledge of the organization, internal auditors are in a unique position to detect fraud early and help avoid or mitigate any fallout by supporting management's efforts to establish a culture that embraces honesty, ethics, and integrity. Ia

NORBERT TSCHAKERT, PHD, CIA, CPA, CFE, *is the Gassett-Schiller '83 Associate Professor of Accounting at Salem State University in Salem, Mass.*

BELVERD NEEDLES JR., PHD, CPA, CMA, GCMA, *is the EY Distinguished Professor of Accountancy at DePaul University in Chicago.*

MARK HOLTZBLATT, PHD, CPA, *is an associate professor of accounting at Cleveland State University.*

BY MATT SUOZZO EDITED BY MARK BRINKLEY

ANTICIPATING INFORMATION SECURITY REGULATION

As threats and data breaches become more common, so will regulatory oversight.

Anyone who keeps up with current events couldn't miss the almost constant stream of articles about organizations, of all types and sizes, that have experienced security breaches resulting in the exposure of customer information. Regulatory bodies and government agencies have taken notice, as well, and have increased their efforts to enforce existing security guidelines, improve guidance while increasing expectations, and develop new requirements and objectives. U.S. organizations in the banking, health-care, and government sectors have long faced security-related regulatory requirements through the Gramm-Leach Bliley Act, the Health Insurance Portability and Accountability Act, and the Federal Information Security Management Act (FISMA). As threats evolve and data breaches become more commonplace, regulatory oversight and enforcement is spreading to other industries. Recent enforcement activities by U.S. bodies such as the Securities and Exchange Commission and Consumer Financial Protection Bureau (CFPB) appear to be signs of things to come.

For example, in March 2016, the CFPB assessed its first data security-related fine against an online payment platform. The CFPB stated that the organization misrepresented its controls and practices around data security, assessed a US$100,000 penalty, and required that the organization address its security practices. According to CFPB Director Richard Cordray, "With data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." This was the CFPB's first enforcement action in the data security space and put many organizations on notice.

Most organizations likely have some form of security controls and processes in place, but those might not always measure up to current industry accepted best practices. There are certain processes and controls that organizations in any industry should consider in anticipation of increased regulatory scrutiny.

Establish a Security Risk Assessment Process The risk assessment is the basis for building and implementing sound information security processes and controls. The traditional approach to information security has been compliance- or rule-based. Taking a risk-based approach is more effective for anticipating where regulatory controls are heading. If organizations do not adequately assess their risks, how can they ensure security controls are implemented to protect their most critical assets?

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

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

There are many different approaches to performing a security risk assessment. Usually, organizations will develop an inventory of their assets, catalog where sensitive data resides, and identify potential threats. Each asset is assigned an inherent risk score based on the criticality of the data that is accessible from it. Next, organizations identify the potential avenues for an individual or organization with malicious intent to gain access to the highest risk assets. The organization then identifies what controls or processes are in place to mitigate the identified threats. Where gaps in controls exist, the organization evaluates the cost/benefit of either implementing new mitigating controls or processes or changing existing practices to remedy the issue.

With the ever-changing landscape of security technology, regulatory requirements, threats, and vulnerabilities, the security risk assessment should be performed regularly, and as necessary, based on significant changes to the organization. Most organizations perform assessments either annually or semi-annually, depending on industry and risk tolerance. The risk assessment should be repeatable and well-documented to allow for consistent reporting of results and comparison over time. The results of the risk assessment should be documented and communicated to management and other stakeholders (e.g., legal, compliance) to aid in decision making.

Develop/Enhance the Information Security Program For organizations that want to anticipate future regulatory requirements, adopting an industry accepted security standard is a solid foundation upon which to build. Frameworks include ISO 27001, U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, FISMA, various aspects of COBIT, and the IT Infrastructure Library, among others. One size does not fit all. For example, if an organization adopts NIST 800-53 as a framework, which is comprehensive and applicable to most government agencies, all of the requirements may not be reasonably implemented based on the organization's risk profile. Organizations should evaluate the framework of choice and map controls to the existing environment. Where there are gaps, management should evaluate the risk exposure and determine action plans in alignment with risk tolerance and overall objectives.

Once the necessary information security controls have been identified, and potentially implemented, the organization should either document or update its security program. This document serves as the foundation of information security processes and practices throughout the organization, and most likely would be one of the first documents a regulatory body would request. The document should describe the governance structure, including policies, and various controls and processes that help mitigate security related risks.

An organization can spend unlimited resources on the most cutting-edge security technology, but if it can be bypassed by an employee accidentally providing credentials or compromising a workstation by clicking on a malicious email link, then it is all for naught. Implementing an employee security awareness program is paramount to the success of a security program. Employees should be educated, tested, and continuously reminded about current security threats and best practices to minimize the effectiveness of social engineering.

Validate the Control Environment Upon implementation of the security program and its supporting processes and controls, organizations should develop a process to periodically assess and validate the control environment. Most organizations with an internet presence are being scanned and assessed by attackers, either manually or via automated scanning, daily. Organizations should strive to stay one step ahead by performing their own assessments, which often include automated vulnerability scanning and penetration testing.

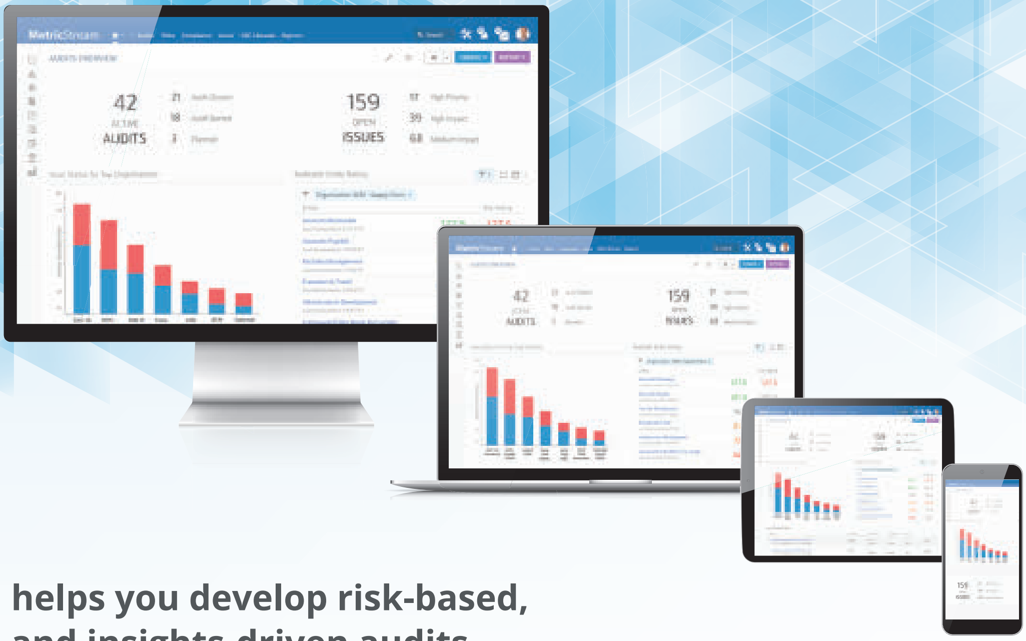
Nontechnical controls such as policy, procedure, and risk assessment processes also should be assessed periodically to determine whether they are being performed in accordance with the established security program. It is common for processes to be defined and then fall behind due to factors such as changes in leadership or competing priorities. By performing validation activities, an organization can demonstrate that it has established an effective security program and that it also regularly reviews its environment to ensure it stays abreast of changes in the security landscape.

Organizations may be preparing for security requirements that have not yet been defined. By performing a security risk assessment, adopting an industry accepted security framework, and implementing and validating the effectiveness of security controls, an organization can position itself to not only decrease the risk for itself and its customers, but also minimize the impact of new legislation and regulatory requirements. Organizations should monitor the ever-changing security threat and regulatory landscape and attempt to anticipate any processes or controls that are not currently part of their program. Also, organizations should monitor the laws in the states and countries in which they operate, or in which they intend to expand, to ensure that guidelines are understood and implemented in the security program. When it comes to information security, both from a regulatory compliance and a technical control perspective, it is more effective to stay ahead of the curve than to work from behind it. Ia

MATT SUOZZO *is an associate director in Protiviti's IT Consulting and Internal Audit practices in Overland Park, Kan.*

MetricStream

Streamline, Simplify and Strengthen Audits



**MetricStream helps you develop risk-based,
collaborative, and insights-driven audits
that take your business to new heights of success**

Prioritize and plan audits

Enhance real time visibility

Optimize resource utilization

Effectively remediate issues

Strengthen audit reporting

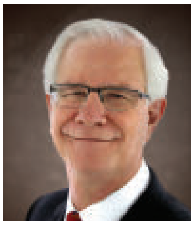
Improve audit performance

MetricStream

Better Information, Better Decisions.

Contact :
www.metricstream.com, Phone: + 1 650 620 2955, E-mail: info@metricstream.com

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



BY J. MICHAEL JACKA

KEEP YOUR PROMISES

Internal auditors are only as good as their word.

Recently, I saw a sign in a hotel elevator that said, "Your satisfaction is more than a goal, it's a promise." It was just one in a slew of aphorisms that seem to permeate today's customer-focused environment. However, this one caught my eye because it made an interesting distinction—goals versus promises.

Consider some of the stated (and unstated) goals internal auditors establish with customers. At the outset of an engagement we talk to them about what we will accomplish, what we need from them, and what they can expect in return. Generally, the discussion results in goals like providing immediate updates on issues and concerns, getting the customer's input throughout the process, and using the customer's time efficiently. It also usually results in specific timelines for the ongoing completion of the engagement.

However, we underestimate the significance of this customer interaction if we think of the agreed items as simply goals. They are promises—and this is not a trivial distinction. Goals are aspirational; promises (if your word actually means anything) are immutable.

Take, for example, the date the report will be issued. How often is the final report actually issued on the date agreed upon at the outset of the audit? Does it often occur on a revised date? Maybe the testing takes longer than anticipated, or the client goes on vacation, or certain interviewees are unavailable, or more report rewrites are required than expected, or (fill in the blank with your favorite reason/excuse). Besides, the customer is often consulted and everyone agrees on the revised schedule, right?

I'm sorry, but poor planning is not a viable excuse for going back on a promise. And if every audit engagement includes breaking a promise as simple as the date of final report issuance, what is the customer to think about all those other promises? "You say there will be open communication, but how often will I be surprised by something? You say you will keep me advised on progress, but how often will periodic updates be cancelled? You say you will use my time efficiently, but how many times will my staff and I answer the same questions and provide the same information?"

In my former role, my team provided the audit customer with a document that specified, among other items, the background, time frame, and scope of the upcoming audit. Externally it was called the Terms of Condition. Within my group we called it our contract. It represented a binding agreement with, and promise to, our customer.

Internal auditors are only as good as their word. And it is a slippery path to begin saying there are extenuating circumstances that mean we can go back on that word. Something as simple as a report issuance date can be the start of that slide, and it should be viewed as a serious breach of commitment. Ia

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

READ MIKE JACKA'S BLOG visit InternalAuditor.org/mike-jacka

NOT JUST A MANUFACTURER RISK

Environmental, health and safety (EH&S) risks can be found in every type of organization.

SCOTT ROIS, CPEA
Member
IIA EHS Advisory Board

DOUG ANDERSON, CIA, CRMA
Managing Director
IIA CAE Solutions

Are there EH&S risks that are applicable to all organizations?

ANDERSON EH&S risks are there; auditors just have to open their eyes. Health and safety affect every company with employees whether it is travel safety, internal building climate, or carpal tunnel syndrome. The challenge is to make sure internal audit considers the broad range of EH&S risks during its ongoing risk assessment. The auditor can't assume there are no high EH&S risks just because the organization isn't a manufacturer of dangerous products.

ROIS Any commercial enterprise has EH&S risks. Large air-conditioning systems on buildings must be tested and repairs documented. Backup generators are usually fueled by underground storage tanks subject to multiple requirements. Modern computer systems have battery backup systems where both environmental and safety regulations apply. Spent fluorescent light bulbs are regulated as universal waste. Fire suppression systems that use halon are regulated, as are inspections and testing of fire extinguishers. Something as basic as a fire hose has multiple construction, storage, inspection, and test requirements.

Are most EH&S risks compliance-related and independent of other risks?

ROIS If you ask EH&S professionals about risk, they will initially talk about their compliance footprint. But if you ask about management of change, they'll quickly agree that change is a real and ubiquitous risk. One of the most common changes is personnel turnover; it can arise from either external business disruptions or internal organic growth. In either case, personnel changes will cause a system to reset. Other intertwined risks include undefined expectations, lack of knowledge, and misaligned incentives. EH&S compliance risk is absolutely tied to all of these risks and all other operational risks.

ANDERSON While EH&S matters are often covered by laws, rules, and regulations, this doesn't mean EH&S risks are only compliance-related. Many risks are a combination of operational, financial, strategic, and compliance. For example, the risk of poor discipline in operating a manufacturing process can generate waste. Waste is expensive and represents an operating risk. Waste also can be a hazardous material, meaning it is now a compliance risk. Ensuring waste is reduced accomplishes both an operational and compliance objective. Similar connections exist between compliance and reputational risks or compliance and financial reporting risks.

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

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

How do you assess the importance of EH&S risks?

ANDERSON Like many risks, EH&S-related risks can be complex. Assessing their importance will often require more than a simplistic understanding of the amount and likelihood of fines that could be levied by a governmental agency if a regulation is violated. The first step — beyond identifying the EH&S risk — is holistically considering the risk's impact to the organization. EH&S risks frequently impact operational, reputational, compliance, and even strategic objectives. For each of these impacts, the auditor should consider the nature and extent of the impact along with other characteristics that define the risk — for example, velocity on onset and longevity of impact. Of course, the importance of EH&S matters to the overall success of the business would likely be paramount, but other impacts can add up.

ROIS An EH&S failure can affect the environment, safety, product quality, and product stewardship. An EH&S failure can also go beyond regulatory requirements and affect brand image and company reputation. The most successful EH&S programs are integrated with overall operating programs that combine common elements. Common and baseline controls like training, inspections, monitoring, and audits can address many of the same root causes. So EH&S risk is not separate from other risks and can cause or be caused by those other types of risks. Success comes when the risks and controls are considered thoughtfully and systems are designed to address the total risk.

Is auditing EH&S risk management different from other auditing?

ROIS It is not different from other management system audits, but it is very different from a compliance audit. Like all audits of management systems, it requires experienced and knowledgeable auditors. All mature audit programs move from compliance, to management systems, and ultimately focus on risk. When internal audit considers risk management, auditors need to address questions that are more nuanced, like leadership commitment, employee involvement, incentives, risk identification, knowledge sharing, and management of change. While there are yes/no questions in a management systems audit, they call for subjective judgments by a skilled and experienced audit team.

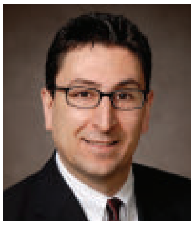
ANDERSON Internal auditing is a profession with clear disciplines and attributes that impact its success. In that way, EH&S auditing is not unique. In addition, most auditors use common methods of obtaining information and analyzing it. The differences most likely fall into documentation and reporting, and these can be significant differences. For internal auditing, there are the well-recognized *International Standards for the Professional Practice of Internal Auditing*, but the standards specific to EH&S auditors are not as well known. Some of the differences in the way EH&S audits are conducted may come from the differences in standards. Other differences likely come from different regulatory environments and stakeholders. However, regardless of how practice has developed over the years, the fundamentals are the same — assurance and advice provided through objective, data-driven analysis and insight. Adherence to a set of widely recognized standards helps all auditors perform better, and I would hope as the EH&S audit and internal audit communities come closer together, we will all adhere more closely to standards and improve our performance.

Is EH&S audit part of the second or third line of defense in an organization?

ANDERSON I have mostly seen situations where EH&S audit was a part of the second line of defense. As part of that line, these EH&S audit functions had significant levels of expertise, but it can be challenging for them to maintain both the appearance and reality of independence. When the EH&S auditors rotate through this function from the areas they are auditing, or report directly to the people they are auditing — sometimes explicitly, but maybe implicitly — at a minimum, the appearance of independence is challenged. EH&S audit in the second line can be extremely beneficial to an organization. Being able to deliver EH&S expertise throughout the organization from an EH&S audit function can be invaluable. However, every organization needs to ensure that EH&S-related risks are included in the scope of a third line of defense function — internal audit — so independent assurance can be delivered to the board and executive management.

ROIS That is the exact question raised by the U.S. Environmental Protection Agency (EPA) in its recently proposed rule changes to the Risk Management Program rules. The EPA proposed exalting auditor independence (third line of defense) over all other attributes, including internal expertise. In that case, the Auditing Roundtable (now merged with The IIA as the EHS Audit Center) argued that both were possible as long as some administrative controls were in place. Change and regulatory complexity mandate periodic review by subject matter experts. External auditors also see different risks than operating personnel, and they see risks differently. That said, there is a balance point between true independence and leveraging expertise. The balance in each organization will be based on the specific needs of that organization. Ia

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



BY CHRIS DOGAS

THE ULTIMATE LINE OF DEFENSE

Senior management should formally occupy an overarching position of risk oversight and control.

The Three Lines of Defense model for risk oversight and control—which identifies operational management as the first line, risk and compliance functions as the second line, and internal audit as the third—has received considerable attention over the last few years. And while much of that attention has been positive, the model is by no means a perfect solution. In fact, one flaw in particular stands out: Senior management, while assigned oversight responsibility for the three lines, does not itself occupy a line of defense. Yet company officers actively own and operate several key controls, shape organizational culture, influence the control structure, establish corporate governance, and may be held liable by regulators for financial fraud and ineffective compliance programs. The senior management team should not only occupy a defense line, it should be considered the ultimate line of defense.

Through its positioning and specific activities, senior management plays an essential role in the organization's internal controls. Indeed, company-level controls are routinely handled at the highest organizational level. Examples include setting operating objectives and targets, approving strategic plans, and signing off on financial and tax filings. Senior management's involvement in these mechanisms is integral to overall control effectiveness.

Corporate culture and tone at the top, also areas of senior management responsibility, maintain an important relationship to internal controls—if the culture and tone are weak, the internal control structure will likely be ineffective. Senior management, of course, sets the tone at the top and plays a large part in establishing a healthy culture. For these areas to function well, senior management must not only possess the highest level of diligence, duty of care, and ethics, but it must also project exemplary leadership.

Senior management's role is also paramount in achieving effective governance. By way of organizational configuration and correct resource allocation, it needs to establish sufficient checks and balances and appropriate independence to foster transparency and objective decision-making. Its role and influence are manifested in areas such as balancing the demand for productivity, growth, and bottom-line results with the need for a steady moral compass and sound ethical practices; making senior leader hiring decisions; and establishing the structure of organizational reward systems.

To serve as an effective contributor, senior management needs to play an active role in governance, risk, and control. The Three Lines of Defense model therefore appears incomplete without formal inclusion of senior management as one of its dedicated lines. Assigning senior management as the ultimate line of defense will strengthen the model's effectiveness and task senior management with formal control ownership. It will also help internal auditors and other assurance providers ask tough questions and engage in more qualitative conversations on governance, risk, and control. Ia

CHRIS DOGAS, CRMA, CPA, CFE, *is head of finance transformation and compliance for a large global company in Boston.*

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