INTERNAL AUDITOR

FEBRUARY 2017

INTERNALAUDITOR.ORG

Core Principles and the QAIP

The Ethical Auditor

A Phased Approach to IT Integration

Breaking Down the *Standards*

AUDITING WHAT MATTERS

Internal auditors who want to be seen as trusted advisors need to ensure they're capturing what matters most to the business.

L.I.V.E. THE GLOBAL EXPERIENCE

LEADERSHIP. INNOVATION. VALUE. EFFECTIVENESS.

Join us Down Under in Sydney, Australia for The IIA's International Conference, 23–26 July 2017.

With an innovative program customizable to training needs, this premier event provides an engaging journey, rich with insights for internal auditors at every level.

Network with 2,000+ peers from over 100 countries as you immerse yourself in 70 dynamic sessions and this eclectic international city.

Choose from sessions in ten educational streams focused on emerging global issues; tools and technologies; innovation in practice management; social business engagement; financial services; risk management and adding value; delivering value to the community in public sector; and more.

CONFIRMED KEYNOTE SPEAKER:

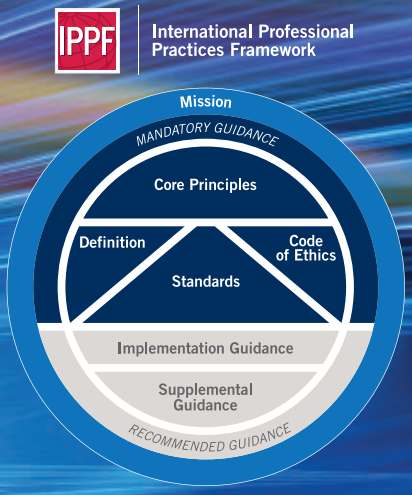
Jonathan Calvert
Editor, Author, Insight Investigations Team, The Sunday Times

As the longest serving editor of the Insight Investigations Team, Calvert has led his reporters through many exclusives – including the FIFA investigation – and even co-authored a book on the scandal. He has won numerous awards, including Journalist of the Year at the British Press Awards.

Register early and save up to AUD$200!
Visit **ic.globaliia.org** for details.

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
SYDNEY, AUSTRALIA / 23-26 JULY 2017
SYDNEY2017

2017-1132



New 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 *International Standards for the Professional Practice of Internal Auditing* and **Supplemental Guidance** provides detailed processes and procedures.

Implementation Guides

New implementation guidance is available to support newly updated standards:

- IG1000 Series
- IG1100 Series
- IG1200 Series
- IG1300 Series
- IG2000 Series
- IG2100 Series
- IG2200 Series
- IG2300 Series
- IG2400 Series
- IG2500 Series
- IG2600 Series

Supplemental Guidance

- Audit Reports: Communicating Assurance Engagement Results

Global Technology Audit Guide (GTAG)

- Understanding and Auditing Big Data

*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.

The Institute of Internal Auditors | Global

2017-1588

INTERNAL AUDITOR

FEBRUARY 2017 VOLUME LXXIV: I

FEATURES

Deloitte.

Drive insights

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

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

www.deloitte.com/us/internalaudit

INTERNAL AUDITOR

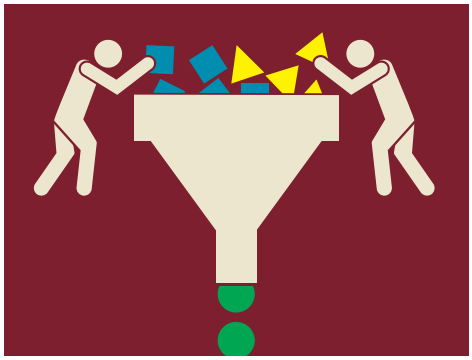
FEBRUARY 2017 VOLUME LXXIV: I

DEPARTMENTS

PRACTICES

INSIGHTS

ONLINE InternalAuditor.org



From Output to Outcomes Five key steps can help internal auditors play a more proactive role in corrective actions, while still maintaining their independence.

New Leadership, New Risks Regulatory enforcement, political scrutiny, and bank lending are just some of the areas that could be impacted by the new U.S. presidential administration.

On the Hook for Fraud Fraud expert Art Stewart discusses how small retailers can protect themselves from credit card fraud.

Principles of Cyber Oversight A new handbook from the National Association of Corporate Directors promotes cybersecurity guidance for boards.

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: 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. Change of address notices and subscriptions should be directed to IIA Customer Service, +1-407-937-1111. Periodicals postage paid in Lake Mary, Fla., and additional offices. POSTMASTER: Please send form 3579 to: Internal Auditor, 1035 Greenwood Blvd., Suite 401, Lake Mary, FL, 32746, U.S.A. CANADA POST INTERNATIONAL: Publications Mail (Canadian Distribution) Sales Agreement number: 545880; GST registration number: R124590001.

COVER: PHOTO ILLUSTRATION BY SEAN YATES (PHOTOS, BOULE, ALIAKSANDR RADZKO, JULIA KOPACHEVA / SHUTTERSTOCK.COM); THIS PAGE, TOP: MATEJMO / ISTOCKPHOTO.COM, BOTTOM: IGOR KISSELEV / SHUTTERSTOCK.COM

Your Team's Only as Great as Their Goods.

Do You Have Your Team Development Roadmap?

The IIA's Team Training group provides tailored, flexible, and affordable team development plans that focus on seven important steps on the continued road to success. Let us help identify your current internal audit training needs and future audit team goals, as well as monitor your progress to drive proven and lasting results.

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

**Training session must be under contract by March 31, 2017, to redeem an IIA Learning OnDemand course offer.*

The IIA Team Development
www.theiia.org/TeamDevelopment

The Institute of Internal Auditors

2017-1624

TOOLS OF THE TRADE

Although the practice of internal auditing is more complex and the expectations of auditors greater than ever, the foundation of the profession—The International Professional Practices Framework (IPPF)—remains strong and continues to provide the foothold internal auditors need to be successful. *Internal Auditor*'s first issue of 2017 begins by considering what matters most to today's organizations and then reminds internal auditors of the tools they should be using, like the IPPF, to ensure a consistent and professional approach to addressing those issues.

As author Jane Seago says in our cover story, "Auditing What Matters" (see page 22), "in any business, time and resources are limited, and internal auditors who want to serve as trusted advisors to the organization must ensure their efforts provide maximum return on investment." In other words, internal auditors need to make sure they are auditing the right things. "An initial key step in elevating to be a strategic partner is understanding the organization's strategic mission, the objectives designed to accomplish that mission, and the metrics by which success will be measured," says Luz Dary Bedoya Bedoya of Audilimited, Organización Corona in the latest IIA Global Perspectives and Insights report, Elevating Internal Audit's Strategic Impact.

Basing their work on the *International Standards for the Professional Practice of Internal Auditing* is a must. However, in the 2015 Common Body of Knowledge report, Looking to the Future for Internal Audit Standards, only 54 percent of CAEs surveyed used all of the *Standards*, with 11 percent reporting they did not use any of the *Standards*. Although an improvement on the numbers reported in 2010—46 percent and 14 percent, respectively—the findings indicate internal audit has a ways to go.

I wonder, however, whether those who say they don't use the *Standards* are actually following the guidance, but are unaware they are doing so. In "Breaking Down the Standards" (page 50), Christine Hovious, director, IIA Global Standards and Guidance, acknowledges that "The phrase 'conformance with the *Standards*' can sound authoritative and overwhelming, suggesting a complex, resource-intensive effort." But, she explains, conformance is much easier to achieve than many CAEs may believe. "In fact, numerous activities performed by practitioners likely conform with the *Standards* already," she says. In her article, Hovious details the components of the *Standards*, breaking them down into bite-size, easily digestible pieces.

The remainder of the February issue delves deeper into the successful practice of internal auditing. From integrated audits, to ethical practice, to auditing governance, to incorporating the Core Principals of the IPPF into quality assessments, we've got you covered on what it takes to succeed in today's organizations.

@AMillage on Twitter

Reader Forum

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

The Slow Pace of Diversity

I am currently a nonpracticing certified internal auditor, having spent several years over internal audit and compliance for a health-care system. As I start the descent on a 25-year career in audit and head toward retirement, I, too, share the concerns of Karen Brady ("Healthy Compliance," "Update") regarding personal liability for compliance failures. I read "Growth Through Challenge" and "It's All in the Delivery" and recalled my younger years and the challenges of communication. Honing communication skills is dependent on understanding your audience, including gender bias in communication. It involves not only what we verbalize but our nonverbal cues. It truly is an art that is often left to on-the-job training instead of preparation in a classroom setting.

I subsequently read "Breaking Through," where the last paragraph states, "Although some progress has been made in achieving gender diversity in the internal audit profession, in general, the pace has been slow." When I reached the last page and scanned the photograph for The IIA's 75th year celebration of chairmen and saw that less than 20 percent of those pictured were female, I muttered, "The pace is slow, indeed." When I am 74, I look forward to a more diverse photograph when The IIA celebrates 100 years.

SHEILA LIMMROTH *comments on the December 2016 issue of* Internal Auditor.

An Educational Issue

There does need to be more information provided to professional athletes, and the general public, on these fraud schemes. Fundamentally, people should always be wary when someone asks for access to bank accounts. A request for access to your bank account, unless it is for a legitimate fixed payment (loan, purchase agreement, etc.) should set off alarm bells in your head.

The penalties for white collar crime definitely need to be strengthened to provide greater deterrents. Also requiring certification and oversight for anyone investing other people's money could help. Otherwise, I don't think this is a government responsibility, but more of an educational issue.

PHIL CASKANETTE *comments on Art Stewart's "NFL Players Tackled by Fraud" (November 2016).*

Priviliged User Failures

Who will guard the guards? Organizations need crystal clear policies regarding who can access what and when.

I am surprised that keeping a laptop allowed the IT technician to continue the scheme. I can see a lot of things that went wrong.

- The laptop was not sanitized.
- Access rights were not deleted.

Ia
INTERNAL AUDITOR
FEBRUARY 2017
VOLUME LXXIV:1

EDITOR IN CHIEF
Anne Millage

MANAGING EDITOR
David Salierno

ASSOCIATE MANAGING EDITOR
Tim McCollum

SENIOR EDITOR
Shannon Steffee

ART DIRECTION
Yacinski Design, LLC

PRODUCTION MANAGER
Gretchen Gorfine

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")

MORE VISIT InternalAuditor.org for the latest blogs.

- There were no granular rights to folders or devices.
- Employee access to the internet was not monitored.
- The internal network and internet-facing devices were not segregated or fire-walled.

I hope the company learned a valuable lesson and implemented appropriate controls to monitor the activities of privileged users.

MANOJ AGARWAL *comments on "The IT Guy" (InternalAuditor.org, January).*

Break the Mold

Great article, Richard, with five great points. No. 2, talent management, is one I find quite important, yet I find it's the least appreciated by management. It will be nice to know how our profession can change that and break the mold.

ROGER NGONG *comments on the Chambers on the Profession blog post, "5 Resolutions for Internal Auditors in 2017 to Prepare for the Future."*

Heat Maps Don't Show the Whole Story

I agree with [Norman Marks] that heat maps fail to show the entire picture. Sure, they map out risks according to their rating, but that's not the whole story and it can be grossly misleading. There may be, for example, a large number of red high risks and relatively few low ones, but that may be acceptable, given the organization's risk appetite and its tolerance for specific risks. Similarly, a large number of deceptively reassuring green low risks may look comforting, but if they reflect very low likelihood but high consequence catastrophic risks, or are simply beyond the tolerance of the organization, they may still need urgent action. Boards may like their simplicity, but heat maps really aren't adequate for communicating complex risks to decision-makers.

CHRIS MACLEAN *comments on the Marks on Governance blog post, "What Does the New Year Hold for Internal Audit?"*

Ready to help you manage risk and realize opportunity, with local presence and global reach delivered through our Business Risk Services capabilities.

Grant Thornton | Audit | Tax | Advisory | **grantthornton.global**

Gaps in ability to use budget data... Top risks raise uncertainty globally... Expectations for new U.S. president... Supply chains face deforestation risk.

Update

THE CYBER RESILIENCE CHALLENGE

IT officers cite weaknesses in breach recovery efforts.

Executives worldwide say they are confident in their organization's ability to predict and resist cyberattacks, according to EY's latest Global Information Security Survey. Still, many indicate shortcomings in their ability to recover from an attack.

Half of the 1,735 private-sector IT officers and other executives surveyed say their company could detect a sophisticated cyberattack—the highest level of confidence reported since EY's 2013 survey. Respondents cite their organization's investments in cyber threat intelligence, security operations centers (SOCs), continuous monitoring, and active defense systems for building this capability. Nonetheless, 42 percent say they do not have an agreed communications strategy in the event of a significant attack. And while more than half consider business continuity and disaster recovery a high priority, only 39 percent plan to invest more in it during the coming year.

"Organizations have come a long way in preparing for a cyber breach, but as fast as they improve, cyberattackers come up with new tricks," says Paul van Kessel, EY global advisory cybersecurity leader. "[Organizations] need to think beyond just protection and security to 'cyber resilience'—an organizationwide response that helps them

EMERGING THREATS

U.S. public company board directors say five risk factors will have the greatest impact over the next 12 months.

1. **60%** Global economic uncertainty
2. **58%** Increased regulatory burden
3. **53%** Significant industry changes
4. **40%** Business model disruptions
5. **34%** Cybersecurity threats

Source: National Association of Corporate Directors 2016-2017 Public Company Governance Survey

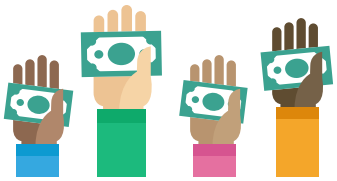
FOR THE LATEST AUDIT-RELATED HEADLINES follow us on Twitter @IaMag_IIA

PHOTO: MATEJMO / ISTOCKPHOTO.COM

prepare for and fully address these inevitable cybersecurity incidents."

When asked about identifying vulnerabilities, 44 percent of respondents indicate that their company does not have an SOC to continuously monitor for cyberattacks, and 55 percent either do not have vulnerability identification capabilities or have only informal capabilities. More than half say they experienced a significant cybersecurity incident in 2016, and 48 percent cited outdated information security controls or architecture as their highest vulnerability—an increase from 34 percent in the 2015 survey.

Respondents identified their top cybersecurity threats: malware, phishing, theft of financial information, and intellectual property theft. Moreover, the top obstacles facing their information security function—budget constraints, lack of skilled resources, and lack of executive support—are virtually unchanged from last year. **—D. SALIERNO**



US$1 trillion
is estimated to be paid in bribes worldwide each year.

The poor pay up to
13 percent
of their incomes in bribes—the highest percentage of any income level.

"The harm that corruption causes to development is, in fact, a multiple of the estimated volume, given the negative impact of corruption on the poor and on economic growth," The World Bank says.

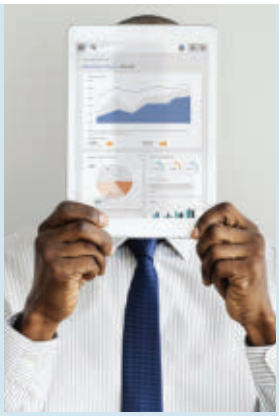
Source: The World Bank November 2016 anti-corruption brief

BUDGETS OUT OF VIEW

Research looks at the demand side of government transparency.

New research finds a gap between the growing amount of budget information that governments of developing nations are providing to the public and the capacity of organizations to use that information. For its report, How Does Civil Society Use Budget Information?, the International Budget Partnership surveyed 176 respondents in 70 countries representing civil society organizations (CSOs) such as advocacy groups and public policy think tanks.

A glaring example of a gap is the low use of audit reports by CSOs across all regions. Audit reports are most used in the Eastern Europe/Central Asia and South Asia regions (36 percent), while they are least used in sub-Saharan Africa (14 percent).



Making all types of fiscal data more accessible could enhance transparency, the study suggests. This could be done by standardizing the formats in which data is released, and consolidating information on web portals. **—T. MCCOLLUM**

GLOBAL UNCERTAINTIES

Executives say economic conditions, regulation, and other top risks pose greater threat.

Business executives say they are most concerned that economic conditions in the markets their organization serves will inhibit its growth opportunities in 2017, putting it first among the top 10 risks reported by Protiviti Inc. and the Enterprise Risk Management (ERM) Initiative at North Carolina State University. Seventy-two percent of the 720 executives surveyed say the potential impact on their organizations of recent global uncertainties are a greater risk than in previous years, according to Executive Perspectives on Top Risks for 2017.

Scores for the top 10 risks are higher than in the 2016 report, reflecting a shift

TOP: NATALI LI / SHUTTERSTOCK.COM; RIGHT: RAWPIXEL.COM / SHUTTERSTOCK.COM; LEFT: LIGHTSPRING / SHUTTERSTOCK.COM

"in the focus of board members and C-suite executives toward risks associated with international and domestic economic conditions, regulatory scrutiny, and cyber threats," says ERM Initiative Director Mark Beasley.

Indeed, regulatory changes and heightened scrutiny from regulators is the No. 2 risk, cited by 66 percent of respondents. The third rated risk is ability to respond to cyber threats that could disrupt operations or damage the organization's brand (60 percent).

Rounding out the top 10 risks are disruptive technology, cybersecurity and privacy, executive succession and recruiting talent, market volatility, cultural factors that could impede risk identification, resistance to change, and customer retention.

Despite heightened concerns about the top risks, organizations may not be taking sufficient steps to address them. Beasley says survey findings indicate "that organizations are not planning to invest additional resources in enhancing their approaches to risk management over the next 12 months." The report notes that respondents' interest in enhancing risk management processes is lower than in the previous two years' surveys. This finding may be because of resource constraints in some organizations or an indication that organizations are satisfied with enhancements made in previous years, the report posits. **—T. MCCOLLUM**

CHANGING OF THE GUARD

Volatility is on the horizon for internal auditors in the U.S., says Kevin O'Neill, co-leader of Arnold & Porter Kaye Scholer's legislative group.

What compliance trends can auditors expect in 2017?
This will be a year of tremendous change that creates volatility and uncertainty in the internal audit profession. Top political appointees at U.S. regulatory agencies will turn over, and there will be marked changes in priorities with the incoming presidential administration. Those changes in priorities will filter down to the enforcement arena. With a new president who is prone to using social media to provoke policy confrontations with corporations and individuals, there is a material risk that companies may face some negative consequences if they become the focal point of President Trump's attention.

How can a new presidential administration affect the risks that organizations face?
President Trump was elected on an agenda to tear down the central legislative, regulatory, and executive actions of his predecessor. There will be a number of recent rulemakings rescinded through legislation, a number of in-progress rulemakings halted or significantly modified, and a number of pending court cases over regulations abandoned to better reflect the new president's priorities and philosophies. It will be critical for internal auditors to stay aware of the state of play for laws and regulations that most affect their organization's operations on a daily basis.

DEFORESTATION RISKS UNDERESTIMATED

Unsustainable commodities increase pressure on supply chains.

Up to US$906 billion in annual revenue could be at risk as a result of nearly a quarter of global company sales depending on four commodities linked to deforestation, according to the Carbon Disclosure Project's (CDP's) report, Revenue at Risk. Fewer than half (42 percent) of companies surveyed have evaluated how their growth strategy will be impacted by the availability and quality of these commodities—cattle products, palm oil, soy, and timber products—over the next five years.

"Companies need to address the sustainability of products that drive deforestation quite simply to protect their balance sheets," says Katie McCoy, head of forests at the CDP, a London-based global disclosure system for investors, companies, and governments to manage their environmental impacts. "If unsustainable commodities enter

the top of a supply chain, the effects will cascade throughout."

Though 72 percent of respondents say they are confident they will be able to source these supplies sustainably, only 44 percent of respondents with procurement standards monitor compliance with these standards and audit suppliers. The CDP calls for companies to ask for transparency and disclosure from their suppliers. **—S. STEFFEE**

RIGHT: MOPIC / SHUTTERSTOCK.COM

Back to Basics

LAL BALKARAN EDITED BY JAMES ROTH + LAURA SOILEAU

DATA MINING

By leveraging data, internal auditors can address issues beyond the reach of traditional analysis techniques.

The vast amount of data generated by business and the increase in data warehouses and legacy systems have created a treasure trove of information to be mined to draw meaningful insights regarding fraud indicators, emerging risks, and business performance. Companies such as Amazon, Facebook, Google, and Netflix are built on foundations of data exploration and mining.

Data mining, which includes text mining, is the discovery of information without a previously formulated hypothesis where relationships, patterns, and trends hidden in large data sets are uncovered. It involves using methods at the convergence of artificial intelligence, machine learning, statistics, and database systems. With the advent of big data, this niche-driven research discipline, developed in the 1980s, is now a powerful tool.

There are no roadmaps or directions in data mining. Instead, it requires thinking outside the box to come up with a range of scenarios. Questions like, "What are the risks?" "What opportunities exist for business improvements?" "How can this data be leveraged?" and "What fraudulent activities can occur?" can lead to developing algorithms.

Data Mining Techniques

The most common techniques used in data mining are predictive modeling, data segmentation, neural networks, link analysis, and deviation detection.

Predictive modeling uses "if then" rules to build algorithms. For example, during a loan audit, auditors can create rules to show which customers in a specific age range (18-25, for instance) with balances exceeding US$5,000 are likely to default.

Data segmentation involves partitioning data into segments or clusters of similar records. Also called *clustering*, this technique lets auditors see common factors underlying each segment. For example, a marketing audit can look at residents of urban neighborhoods and affluent areas where wealthier, older people live.

Neural networks are a type of artificial intelligence that uses case-based reasoning and pattern recognition to simulate the way the brain processes, stores, or learns information. In fraud detection, neural networks can learn the characteristics of fraud schemes by comparing new data to stored data and detecting hidden patterns.

Link analysis establishes links between records or sets of records. Such links are called *associations*. Examples include customers buying one product at a specific time and then a different product a few hours later or a vendor supplying a raw material and purchasing a byproduct. Or,

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

EXAMPLES OF DATA MINING

Data mining can detect a range of fraud indicators such as bogus vendors, kickbacks, money laundering, insider trading, and claims fraud.

In a telecommunications audit, for example, a model can be built to show patterns of call destinations, duration, frequency, and time of day. Over time, when actual calls vary from expected patterns, it will alert internal audit to the possibility of fraud.

Outcomes also can indicate cost-saving opportunities, potential irregularities, and patterns worthy of further investigation. For example, in a procurement audit, using text mining that brings up common products and services may determine that there is an annual savings or discount to ordering cleaning supplies from one vendor instead of several vendors.

In a retail audit of a bank branch, a review of customer accounts can show single bank accounts converted to joint accounts, indicating marriage. Internal audit may recommend cross-selling mortgages and consumer loans to the joint account owners, which can grow branch profitability.

In a loan audit, nonperforming loans can be segmented to show different factors for loan failures. This can help guide the revamping of credit models and tightening of lending practices, which can reduce the number of nonperforming loans.

in the case of a money laundering audit, identifying addresses that have many wire transfers attached to them.

Deviation detection is pinpointing deviations from the observations or model worthy of further investigation. An example is detecting an unusual transaction on a credit or purchase card that does not fit the typical spending patterns of a cardholder, such as buying a refrigerator or booking a vacation on a company's purchase card.

Email Mining

The rapid evolution of data mining techniques on unstructured or semi-structured textual data now provides opportunities for audit analysis. Mining this vast text field is a key tool in the internal auditor's arsenal for fraud prevention and detection. Word searches using "kickback," "bank account," "funds," "money," and "override" could uncover fraud, while words such as "flowers," "anniversary," "chocolate," "gift," "bar," and "drink" could indicate office romances that breach a company's code.

Analysis of email logs can uncover key information about employees' interests, activities, and behaviors. Email contents might include potential evidence of fraud and issues of audit concern. For instance, emails from an employee to customers when the employee does not hold a position that normally communicates with customers would be a red flag.

Emails might contain an exchange of information between parties that can provide evidence of a wide range of managerial fraud. Also embedded in email contents might be issues relating to breaches of compliance requirements and their cover ups, privacy matters, and theft of intellectual property. As emails pass through gateways, they are easy to archive, index, categorize, and monitor for keywords.

Social Network Analysis

Analysis of employees' Facebook, Linkedin, and Twitter accounts explores relationships or networks between email senders and recipients. Social network relationships may presage kickbacks or collusion between employees and third parties. Within this context, social media analytics is a tremendous tool. However, consideration should be given to such key risks as security, privacy and confidentiality, loss/theft of intellectual property and trade secrets, and legal and compliance.

Data Mining Tools

Data mining can be performed with comparatively modest database systems and simple tools or off-the-shelf software packages. Microsoft Excel has a wide range of functions that can be used in data mining without the hours of training required for other programs. Generalized audit software and server database software also are formidable data mining tools.

Raising the Bar

Data mining demands considerable time, serious commitment, a new mind-set, and new skills. Delays in getting the data, uncooperative management, time spent understanding the data, and scrubbing it are additional challenges. Data mining raises the bar on what can be achieved by addressing issues beyond the reach of traditional analysis techniques. It is more than running complex queries on large data sets. Internal auditors must work with the data to have it reorganized and cleansed, and identify the format of the information based on the technique or analysis they want to use. Data mining increases audit coverage, and with the internet and computer-assisted audit tools, auditors should be limited only by their imaginations. la

LAL BALKARAN, CIA, FCPA, FCGA, FCMA, *is a risk, governance, and internal audit consultant with LBA Consulting in Scarborough, Ontario.*

BY XIAOHU NIAN, DANIEL X. ZIMMERMAN, + MARY MCCOY EDITED BY STEVE MAR

INTELLIGENT ASSESSMENTS

Government auditors are using cognitive technology to help identify high-risk areas.

Robust audit risk assessments—a key building block of high-impact audits—are, by nature, a challenge for any internal audit department, and even more so in today's dynamic audit environment. Especially in public sector organizations, where limited resources, competing priorities, and lack of subject matter expertise impede risk identification, auditors are increasingly looking to technology for solutions. Specifically, internal auditors can augment their risk management activities by using automated solutions that assess the literature in the field of interest to predict industry trends.

Cognitive technology—intelligent computer systems designed to perform human tasks—has long been used to enhance research and knowledge collection. This technology has potential to transform the internal audit profession, particularly in performing risk assessments.

Auditors at the New York State Office of the State Comptroller (OSC) have developed a tool set that leverages cognitive technology to extract and analyze text from audit reports, creating a search vehicle capable of identifying meaningful data within documents that collectively can help auditors identify high-risk areas. The tool set enables auditors to immediately access a wealth of publicly available, but until recently, elusive audit-critical information, minimizing time-consuming manual processes to identify themes and risks and ultimately improving the effectiveness of risk management, control, and governance processes within the agencies and organizations the OSC audits.

Distilling the Facts

Audit reports represent a source of untapped data. It is difficult to extract value from data using time-consuming manual searches. Conversely, computers have unlimited capacity for extracting value efficiently, as long as document text is prepared in a uniform format that both humans and machines can understand. Applying natural language processing (NLP) to text can allow internal auditors to tap into each sentence of every report, generating mountains of new information. NLP is a field of artificial intelligence that enables computers to understand human language. For example, NLP enables the iPhone's Siri personal assistant to answer users' questions. NLP can transform audit reports into a powerful source of insights for more targeted risk assessments and audits.

Searching for relevant audits requires varying amounts of information to be communicated through a web browser. Audit reports are available on the web in a range of formats—from the simple PDF to the more sophisticated HTML—each with varying levels of interoperability,

depending on how the back-end information is organized. Data can be "structured" text containing additional coded information that facilitates machine reading, or "unstructured" text that lacks the required detail to enable efficient machine reading. The more structured the documents are, the more relevant the document retrieval can be.

The OSC's tool set creates a process to derive machine-readable data from audit reports by: 1) converting text to a standardized structure, 2) adding layers of meaning to the text, and 3) teaching computers to use the information to recognize and understand common audit language, concepts, and themes, as well as to analyze associations. Although the OSC's work to date has involved performance audit reports only, the tool set can be applied to any report type.

The Process

The OSC's tool set uses optical character recognition engines to extract plain text only from each document. We then apply NLP to the plain text. NLP creates additional layers of linguistic information, which allows computers to put words into context and derive meaning.

NLP uses grammar rules to identify and classify parts of speech, and codes them using annotation tags. Likewise, it locates proper nouns, and classifies and tags them according to predefined named entity categories. For example, take the sentence, "For the two fiscal years ended June 30, 2010, the Mill Neck School claimed approximately $16.7 million in reimbursable expenses." NLP identifies and tags "Mill," "Neck," and "School" each as a proper noun singular and then, based on their proximity, classifies and tags the proper nouns collectively as the named entity "organization."

Based on the NLP annotations, additional information extraction techniques detect and tag audit-specific elements such as "auditee" and "finding."

New information derived from NLP annotations allows auditors to data mine every sentence within a collection of documents using a variety of pre-set text recognition "rules" to identify high-relevance themes and risks. These rules, which interact with the computer in the form of user queries, act as filters to guide the computer's recognition of text. Rules can vary in complexity, depending on the type of information the user seeks. For example, users can filter documents based on the frequency of a certain word or word combination occurring within them (visually represented as a word cloud) or on a cluster of specific words that are commonly associated with a given audit concept such as a finding.

Using the criteria of a given rule, the computer can search a database of annotated documents and identify text that fits the rule. For example, if auditors are interested in identifying areas within the Medicaid program at risk for overpayment, they can query the database for the word combination "overpayment–Medicaid." The tool set then analyzes all the reports in the database, identifies those that contain the "overpayment–Medicaid" word combination, and ranks them by frequency of word combination occurrence.

After auditors select the reports that are of interest, the computer can automatically extract audit concept information from each. For example, certain words such as "ensure," "need," "reveal," and "discover" are frequently used in reports' findings sections. The computer searches for these words and extracts sections from the reports that contain them. Information can be retrieved in source list or text display views. As the computer's knowledge bank grows—by learning new queries, understanding them in the context of existing queries, and thus creating new knowledge—the technology will become increasingly intuitive of the user's intent.

Risk Assessment Transformed

Applied to the OSC's growing database of audit reports, the tool set has transformed the office's risk assessments by:

- Unlocking new insights from raw information in existing work, which expands the scope of risk assessment.
- Speeding data collection.
- Enabling auditors to assess the quality of data faster and determine which are most useful.
- Allowing auditors to leverage real-time data to continuously monitor trends and more quickly identify new risks.

As a result, the OSC's auditors are better equipped to identify threats to a program's or an organization's success and sustainability, conduct more productive audits, make meaningful recommendations, and ultimately deliver on their professional commitment to improve governance, operations, risk management, and control processes.

Adapting to Changing Risk

The audit environment of today is highly dynamic: Risks are increasing in number and complexity, as are the number of regulations being created to control them. The OSC's tool set is a critical resource to help auditors adapt to these changes, while supporting the profession's advocacy of good governance. It's an example of how internal auditors globally could leverage the benefits of technologies such as artificial intelligence to address risk in real time. IA

XIAOHU NIAN *is a research assistant at the New York State Office of the State Comptroller in Albany.*

DANIEL X. ZIMMERMAN *is a research analyst at the New York State Office of the State Comptroller.*

MARY MCCOY *is a senior editor at the New York State Office of the State Comptroller.*

BY STEVE MORANG EDITED BY PAUL SOBEL

TURNING UP THE HEAT ON FRAUD

A fraud risk assessment can help auditors take the organization's ethical temperature.

Conducting a fraud risk assessment is an important step for internal auditors who are evaluating an organization's internal control environment. As part of these assessments, practitioners can use surveys, focus groups, and workshops with employees to take the organization's ethical temperature and determine its ethical baseline.

Conducting a fraud risk assessment is similar to an internal audit risk assessment exercise carried out during the audit planning process, but the focus is specifically on fraud risk. The most successful fraud risk assessments are conducted in small brainstorming sessions with the operational management of the area under discussion. Facilitated by a fraud professional such as a Certified Fraud Examiner or internal auditor with appropriate fraud training, these assessments look at typical fraud schemes found in various areas of the organization and identify the internal controls designed to mitigate each of them. At a high level, this analysis examines internal controls and the internal control environment, as well as resources available to prevent, detect, and deter fraud.

A Different Assessment

A fraud risk assessment evaluates areas of potential fraud to determine whether the current control structure and environment are addressing the fraud risk at a level that aligns with the organization's risk appetite and risk tolerance. Therefore, it is important during the development and implementation of the risk management program to specifically address various fraud schemes to establish the correct levels of control. The Association of Certified Fraud Examiners' Fraud Risk Assessment Tool provides a structured approach to identifying key fraud schemes.

Fraud risk assessments emphasize possible collusion and management overrides to circumvent internal controls. Although an internal control might be in place to prevent fraudulent activity, the analysis must consider how this control could be circumvented, manipulated, or avoided. This evaluation can help the fraud risk assessment team understand the actual robustness and resilience of the control and the control environment, and estimate the potential risk to the organization.

One challenge at this point in the process is ensuring that the analysis assesses not just roles, but specific individuals who are responsible for the controls, as well. Sometimes employees will feel uncomfortable contemplating a fellow employee or manager perpetrating fraud. This is where an outside fraud expert can help facilitate the discussion and ensure that nothing is left off the table. To ask the right questions, the facilitator should keep in mind:

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

- Fraud entails intentional misconduct designed to avoid detection.
- Risk assessments identify where fraud might occur and who the potential perpetrators might be.
- Persons inside and outside of the organization could perpetrate such schemes.
- Fraud perpetrators typically exploit weaknesses in the system of controls, or may override or circumvent controls.
- Fraud perpetrators typically find ways to hide the fraud from detection.

The Ethical Baseline

It's important to evaluate whether the organization's culture promotes ethical or unethical decision-making. Unfortunately, many organizations have established policies and procedures to comply with various regulations and guidelines without committing to promoting a culture of ethical behavior. Simply having a code of conduct or an ethics policy is not enough. What matters is how employees act when confronted with an ethical choice; this is referred to as measuring the organization's ethical baseline.

Organizations can determine their ethical baseline by conducting either an online survey of employees from various areas and levels within the organization, or through workshop-based surveys using a balloting tool that can keep responses anonymous. The broader the survey population, the more insightful the results will be. For optimal results, surveys should be short and direct, with no more than 15 to 20 questions that should only take a few minutes for most employees to answer. An important aspect of conducting this survey is ensuring the anonymity of participants, so that their answers are not influenced by peer pressure or fear of retaliation.

> An organization with a weak ethical baseline may need more frequent audits.

The survey can ask respondents to rate questions or statements on a Likert scale, ranging from 1–Strongly Disagree to 5–Strongly Agree. Sample statements include:

1. Our organizational culture is trust-based.
2. Missing approvals are not a big deal here.
3. Strong personalities dominate most departments.
4. Pressure to perform outweighs ethical behavior.
5. I share my passwords with my co-workers.
6. Retaliation will not be accepted here.
7. The saying "Don't rock the boat!" fits this organization.
8. I am encouraged to speak up whenever needed.
9. Ethical behavior is a top priority of management.
10. I know where I can go if I need to report a potential issue of misconduct.

Interpreting the Results

The ethical baseline should not be measured on a point system, nor should the organization be graded based on the survey results. The results should simply be an indicator of the organization's ethical environment and a tool to identify potential areas of concern. If done over time, the baseline can help identify both positive and negative trends.

The results of the ethical baseline survey should be discussed with management as part of a broader fraud risk assessment project. This is especially important if there are areas with a lack of consensus among the survey respondents. For example, if the answer to a question is split down the middle between strongly agree and strongly disagree, this should be discussed to identify the root cause of the variance. Most questions should be worded to either show strong ethical behaviors or to raise red flags of potential unethical issues or inability to report such issues promptly to the correct level in the organization. For example, if the answer to question 10 is heavily skewed toward Disagree, this could be an area that would need to be discussed to find the root cause. Strong ethical cultures would want a channel for reporting potential issues.

By obtaining a clear snapshot of the organization's ethical temperature at a point in time, internal auditors can re-assess the evaluation of controls beyond purely their design and effectiveness. Instead, they can consider areas that may need additional review.

Bringing It All Together

The results of the fraud risk assessment and ethical baseline survey can help internal auditors determine areas of risk and control that should be considered for upcoming audit projects. For example, fraud risk schemes that are heavily dependent on controls that can be easily overridden may require more frequent assurance from internal audits than those schemes that are mitigated by system-based controls. And an organization with a weak ethical baseline may require more frequent auditing of detective control procedures than one with a strong ethical baseline, which might rely on broader entity-level controls. By measuring their organization's ethical temperature, internal auditors will be turning up the heat on fraud. IA

STEVE MORANG, CIA, CFE, CRMA, *is senior manager–leader advisory fraud & forensics, with Frank, Rimerman & Co. in San Francisco.*

Fraud Findings

BY DONALD K. MCCONNELL JR. + JEAN L. MANUEL EDITED BY BRYANT RICHARDS

THE ACCIDENTAL DISCOVERY

An office manager at a small distribution center tries to cover up her embezzlement scheme.

Pam Hardy, an internal auditor with five years' experience at a large national company, was auditing a remote distribution center when her routine sales and accounts receivable tests revealed minor discrepancies. Because the distribution center was small, it hadn't been visited by internal audit for more than four years. Hardy initially thought that the two-hour drive to the distribution center wasn't worth the time. But when other red flags appeared in addition to the minor discrepancies, Hardy knew she had to look into things further.

Comparing time clock work hours to the temporary payroll agency monthly billings, Hardy found a small difference in actual hours worked and hours billed for one employee. In reviewing personnel files, she also noted that two employees hired for seasonal work didn't have Social Security numbers on file. Hardy learned from the temp agency that it had been trying to obtain the Social Security numbers for these employees, but was told to pay the employees until it could obtain and verify them. Further, Hardy noticed that the emergency contact information for one of the two employees was the same for the remote distribution center manager, Bob Lamp. She later discovered from Sally Wynn, the plant office manager, that the employee was Lamp's son.

Growing uneasy about the circumstances, Hardy decided to review the center's financials. Everything looked fine except that accounts receivable had significantly increased from the prior year. She contacted the corporate office that performed the bank reconciliations to inquire whether there were any issues and was assured that there were none. Hardy was relieved; nevertheless, she was still concerned about Lamp.

Hardy decided to drive to the distribution center the next day to meet with Lamp, but their conversation was constantly being interrupted. Consequently, she suggested that they go to lunch together, but Lamp was unable to attend because of urgent business. He asked Wynn to take Hardy to lunch instead. During lunch, Wynn stated out of the blue that her bank deposits had been consistently late because she was too busy and had to take the deposits to the night drop on her way home. Hardy hadn't asked about the deposits and wondered why Wynn would volunteer that information.

Wynn then explained how difficult it was being a single mother to three children. They would only wear designer clothes, costing more than US$5,000, and they'd recently taken a weekend family trip to Disney World. Hardy also noticed that Wynn drove a luxury automobile. Her

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

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

spending was far above an office manager's salary. Wynn also complained she was so overworked that she never took vacations, only an occasional day off.

As Wynn described her duties, Hardy realized she had total control over cash collections, contrary to company policies. Hardy learned that Wynn was receiving and recording the daily route cash proceeds, preparing daily deposits, taking them to the bank, and entering sales invoices into the accounting system. She was also posting accounts receivable for mailed checks.

Hardy decided to review the cash book. She printed the daily sales reports and copied the cash book for the three months prior. While Hardy was doing this, Wynn suddenly became ill and left for the day, raising yet another red flag. Hardy requested and reviewed the bank reconciliations for the two previous months. She quickly realized they were a recap of the bank statement monthly summary: beginning balance plus deposits, minus disbursements equaling the ending balance. Notably, there was a difference in bank and book cash that hadn't been investigated. There also were no deposits in transit, whereas most locations had at least one. Furthermore, there was no comparison between cash sales and monthly changes in accounts receivable.

Puzzled, Hardy called the accounting clerk who had been doing the reconciliations, who revealed there had been so many problems reconciling the location's cash that she had given up and wasn't reconciling the account. Hardy looked at the difference between the bank balance and general ledger cash and immediately knew there was a problem. There was a difference of almost US$210,000. Analyzing the cash book compared to daily route sales and accounts receivable postings, Hardy suspected Wynn was stealing most of the cash and only depositing checks.

> Some auditors check the boxes but fail to look at the big picture.

The first instance of missing cash occurred about a year before. Hardy surmised Wynn had been lapping accounts receivable payments to cover the theft, misapplying customers' payments to avoid detection. When checks came in the mail, she used them to conceal the cash embezzled from daily route sales, balancing the deposit to daily cash sales. If a customer complained, Wynn always answered the phone, allowing her to shield complaints from Lamp. She also tried to apply payments before subsequent billing dates, hoping customers wouldn't notice the late payment postings.

Hardy confronted Wynn, who quickly confessed, stating she'd experienced financial problems and thought she would borrow the cash, intending to eventually make restitution. However, the longer the scheme went on, the more she believed it would never be detected.

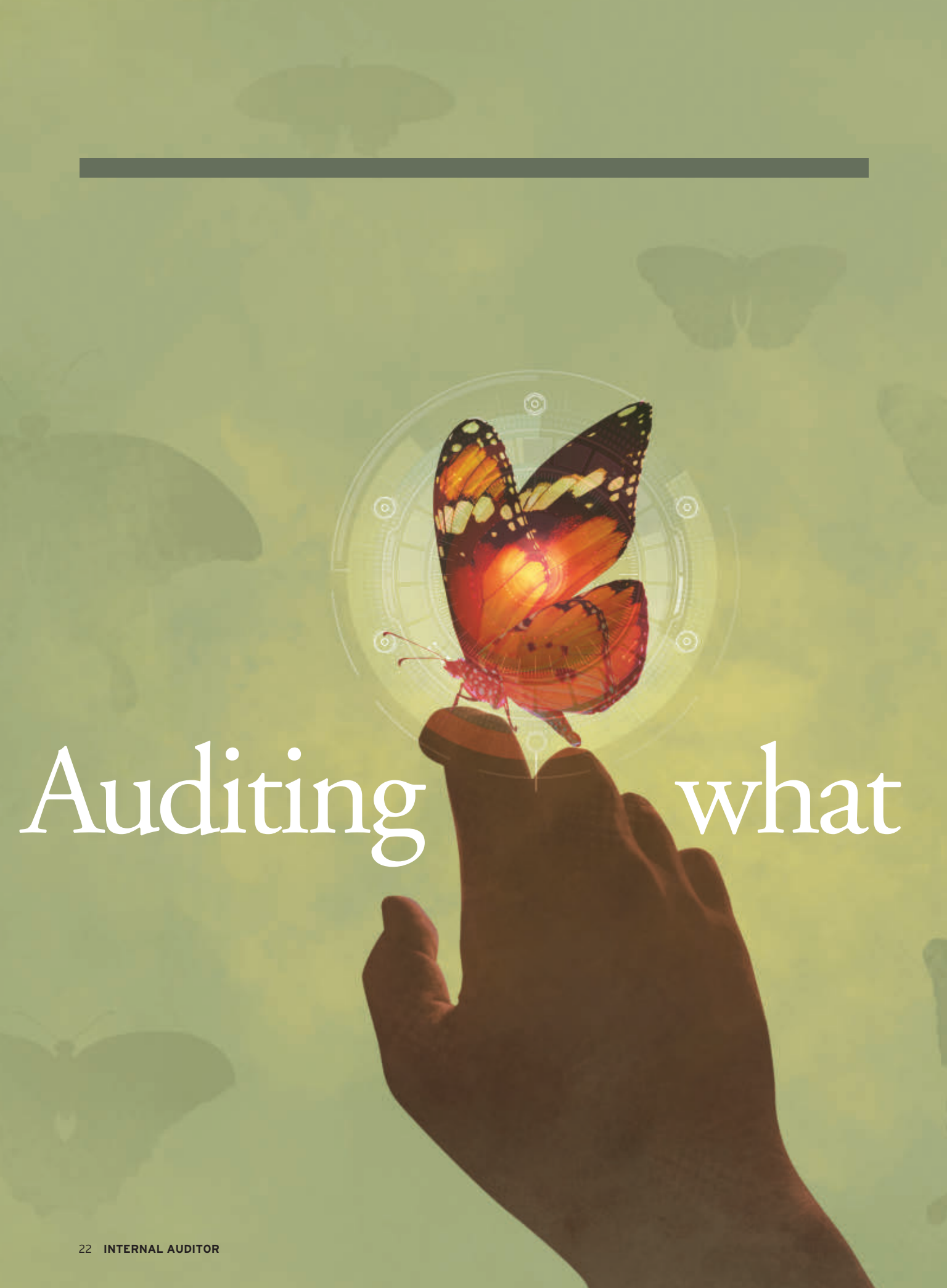
In the aftermath, Wynn pleaded guilty and went to prison for two-and-a-half years. Because Hardy had so thoroughly documented the embezzlement, the insurance company fully paid the dishonesty claim. Corporate corrected the bank reconciliation protocols, and developed electronic exception reports that would immediately identify locations with large cash discrepancies and changes in accounts receivable as a percentage of sales. Further, all personnel were required to take a full week of vacation, at a minimum.

Lessons Learned

- Small or remote locations can be especially vulnerable to embezzlement. Controls consciousness on the part of management can wane in such cases, especially when controls are not audited regularly.
- Don't be afraid to change your fraud hypothesis. Hardy originally thought Lamp might be a fraudster, which led her down the path to Wynn. Lamp's only offense was lack of appropriate controls at his distribution center.
- Wait to confront someone until after the facts have been reviewed. Start by analyzing the underlying documentation. Make a plan regarding which documents need reviewing, who you'll interview, and who needs to be informed about the proceedings. If there is predication of fraud, determine who the most likely suspect is.
- Be flexible and use common sense. Some auditors check the boxes, but fail to look at the big picture. The embezzlement could have been caught sooner if someone had analyzed the change in accounts receivable as a percentage of sales and the large discrepancies between book and bank cash.
- Controls that aren't operating effectively are useless. The accounting clerk hadn't reconciled the location's bank account. Further, the supervisor had signed off without reviewing the reconciliations. Failing to appropriately apply controls can contribute to concealing a theft. la

DONALD K. MCCONNELL, JR., PHD, CPA, CFE, *is a distinguished teaching professor in the Department of Accounting at The University of Texas at Arlington.*

JEAN L. MANUEL, CPA, CFE, CFF, *is a fraud investigator and former internal auditor in Dallas.*



Auditing what

Internal auditors can add value by selecting audits that contribute to achievement of strategic objectives.

Jane Seago

Illustration by Sean Yates

matters

Organizations exist to provide value for their stakeholders, and increasing that value requires businesses to accept appropriate risks. But which risks? And how much uncertainty is too much? To make those decisions, management must evaluate and balance growth opportunities, goals, related risks, and effective deployment of resources, while never taking their eyes off the strategy and enterprise objectives.

Clearly, internal audit has an important role to play in this process. Yet some internal auditors are torn between performing traditional internal audit activities—the time-honored "tick and tie" procedures—and activities that contribute more directly to value creation. "Both those activities are important," says Larry Baker, a senior leader in internal audit, enterprise risk management, and strategic planning in Oklahoma City. "Even when management is convinced the organization is doing everything possible to ensure that a process is working effectively, internal audit still needs to do an independent audit of the controls that make management feel so comfortable."

However, in any business, time and resources are limited, and internal auditors who wish to serve as trusted advisors to the organization must ensure their efforts provide maximum return on investment. Priorities must be set. For some internal auditors, the act of prioritization may necessitate a fresh look at what matters most to the business.

IDENTIFYING THE "RIGHT" RISKS

Bill Watts, partner at Crowe Horwath in Columbus, Ohio, recalls a time more than a decade ago when the approach to determining what to audit was not as thoughtful as it is today. Audits tended to be very structured and

"Determine in advance how the partnership will accelerate business strategy."

Brad Ames

"The important thing is to show where value is created and how it can be affected by certain unwanted events — or enhanced."

Charlotta Löfstrand Hjelm

repeatable. Then came the U.S. Sarbanes-Oxley Act of 2002, which indirectly caused companies to re-examine their control structures and how to improve controls, leading to evolution in other areas. "Internal auditors today must think more broadly, across the enterprise," he notes. "Where is the company strategy focused, what are the major initiatives, and where is the money being spent? Those answers tell you what's important to the entity, and that's where internal audit should focus."

There is yet another question that can help internal audit identify the "right" risks to address, says Brad Ames, internal audit director for Hewlett Packard Enterprise in Palo Alto, Calif.: Who is accountable for a specific strategy? "Once you know that, you can build an authentic relationship with them and make them your stakeholders," he explains. "Ask them what they see that would inhibit them from accomplishing their strategic objectives. Begin the risk discussion, always establishing visibility into risk so they don't overvalue or fear it. Determine in advance how the partnership will accelerate business strategy. This context will help them feel more confident about the risk, making them less likely to allow it to cause them to undercommit to the strategy."

In most organizations, one of the areas of focus will involve technology. All businesses must learn how to optimize the use of technology — not only in any technology-enabled products and services they offer to customers, but also in their own internal business processes for greater efficiencies and effectiveness. Many organizations' strategies include specific objectives related to technology, a clear signal that internal audit must focus on it as well — in Ames' words, "presenting itself as relevant to strategy."

It is also important for internal auditors to recognize that, even as they raise their focus on strategic initiatives, they must maintain many customary audit activities, such as looking at segregation of duties, fraud potential, regulatory compliance, and transactions. However, Ames points out, even the traditional audit activities can and should "move toward strategy."

THE RISK CONNECTION

The upcoming revision of The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management–Integrated Framework*, scheduled for release in early 2017, describes an enterprise risk management (ERM) program that is highly interrelated with controls. Whether internal auditors use COSO ERM to guide their risk-driven strategic activities, or build their own frameworks based on its precepts and shaped by experience and common sense, Watts warns against "cherry-picking activities" from the framework. Focusing only on certain parts of a framework while ignoring others is likely to hinder generating full benefit from the process, perhaps even missing opportunities. Taking a broader, holistic view that aligns the organization's ERM program with strategy facilitates internal audit's understanding of the strategy itself and its role in the major initiatives the business deems critical to accomplish the strategy.

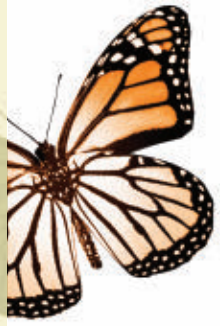
This is not to say that an internal audit focus on organizational objectives, as outlined in the strategy, automatically improves ERM within the organization. "Hopefully it does, but it's far from given," says Charlotta Löfstrand Hjelm, chief internal auditor at Lansforsakringar AB in Stockholm. "If there is no objective, there is no risk. The important thing is to show where value is created and how it can be affected by certain unwanted events — or enhanced, if we

Understanding and **aligning** to the strategic plan helps internal audit offer **meaningful** and relevant assurance. — IIA Global Perspectives and Insights: Elevating Internal Audit's Strategic Impact

MAKING A CASE FOR A MORE STRATEGIC APPROACH

Internal auditors can make inroads into altering their organization's culture to accept a more strategic approach to internal auditing. Here are techniques the audit leaders interviewed for this article recommend to lay the groundwork and prove the department's readiness:

- **Even while performing traditional internal audit activities, have the courage to step outside the norm occasionally.** Be sure to communicate the positive results of the "experimentation" and the ways it benefited the organization. Use that win to build the next one.
- **Take the "journey begins with a single step" approach and start by making one small adjustment.** Then, when the time is right, make another. The key is to take each step with the firm intent of going on the whole journey.
- **Spend more time talking to customers and listen carefully to their responses.** If you are doing a traditional activity such as matching invoices, spend an hour talking to the people who process the invoices. It's often possible to learn more from hearing than seeing, and that knowledge, which may uncover previously unknown issues or opportunities, can help you build a case for expanding internal audit's role.
- **Polish your soft skills.** Those who can ask good questions, establish relationships (within the bounds of independence and objectivity), listen carefully, and summarize succinctly are generally more effective in uncovering truths—and in building compelling business cases for desired outcomes based on those truths.
- **Arm yourself with expertise before acting.** In today's environment, there is a lot of pressure to do more with less, add value, and show productivity. This may cause internal auditors to jump into activities they don't fully understand. Don't make that mistake. Be prepared. Perform research, get training, and ask experts to help you where needed. If you are given a chance to try something new, the odds of getting a second chance will depend on doing the first one well.
- **Don't fear failure.** Not every effort will be a success, but that can't be a reason to give up. Develop your resilience by learning from failure and moving on.



can articulate how to capture this." Showing how goals affect value and risk in other areas can be helpful, as can positioning objectives as the link between the audit plan—including consulting and advisory activities, not only assurance audits—and the different plans from the organization, such as strategic plans, business plans, and risk reports.

Auditors tend to be good at using a risk-focused approach. In fact, Ames speculates that management tends to perceive internal audit as being all about compliance or risk. In his view, a risk-based approach is "our foundation," but internal auditors should be more focused on increasing value to the business, positioning internal audit as partners in strategy.

THE NEED FOR SPEED

A phrase often used to characterize one aspect of the relationship between internal audit and risk management is that internal auditors must "audit at the speed of risk." In today's business environment, types of risk, likelihood of occurrence, and degrees of impact change almost daily. If internal audit is focused on supporting strategic objectives, and if a key factor in accomplishing those objectives is understanding the risk surrounding them, then the speed at which internal audit can identify and act on risk is important. Internal auditors must find ways to remain informed and take proactive measures.

Lisa Lee, vice president, Audit at Google Inc. in Mountain View, Calif., says in a fast-paced environment, the key for internal auditors to add value is to communicate concerns quickly. "Where it makes sense, engaging early with process owners to conduct risk assessments and assess control design effectiveness will help provide clarity on the highest risks that need to be managed," she explains. Moreover, she says, "Assessing the maturity of controls can help provide meaningful information, as manual or detective type controls may be appropriate when a process or product is first

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

FROM CRITICAL OBJECTIVES TO CRITICAL RISKS

Critical objectives often have critical risks. Knowing how to identify those risks, prioritize them, and develop mitigation plans can help internal audit focus its efforts on value-producing activities for the organization. The following process, described by Larry Baker, has been in use at his previous employer, Devon Energy Corp., for many years. Each step is facilitated by internal audit.

STEP 1 IDENTIFY AND DEFINE THE RISKS

- Based on their understanding of the organization's strategic objectives, opportunities, and related risks, senior executives and other management identify major risk areas most important to the company. At Devon, this tends to be approximately 20 risk areas.
- Each risk area's leader defines the risk, details the scope, and identifies two to four inherent risks in that area. The resulting list encompasses between 50 and 60 inherent risks.
- Employees who are knowledgeable about those inherent risks identify factors that drive each inherent risk (control weaknesses), the ERM activities in place to manage the risk (controls), and gaps or opportunities for improvement. They then develop recommendations for how to better manage the risk as needed.

STEP 2 RATE THE RISKS

- Each year, the board, executives, and other management complete a survey on the 20 risk areas. They rate each in four categories: probability, velocity, readiness, and financial impact. Devon's survey is fundamentally the same each year, which enables the company to compare results and trends.

STEP 3 ADDRESS RISK IN DETAIL

- Every quarter, a cross-functional group of vice presidents for three of the 20 risk areas is brought together for a two-hour workshop to focus on the inherent risks for those three areas. The group votes on how effectively the risk is being managed and how effectively it should be managed, then examines the gap between the two results. The gaps are discussed in order of size, largest gaps first.
- The focus is on determining whether there is anything the company should be doing that it isn't doing, or if any new risks are emerging.

It takes approximately 18 months to cover all 20 areas. Internal audit uses these results to identify any new information or changes that need further examination. Significant changes often relate to areas most critical to the organization and, therefore, guide internal audit's effort in valuable, strategic, and risk-driven directions.

launched, but as the process or product matures and scales, so should controls." Using a maturity model, such as a scale from 0 (indicating a nonexistent control) to 5 (indicating an optimized control), can be helpful in instances where there may be a need for more robust controls.

The traditional approach of having an annual audit plan may not mesh well with the speed of today's business. Internal auditors may struggle to adhere to the plan while also trying to accommodate constant change and ensure focus remains on the most critical risks. Lee notes that at Google, internal audit maintains a running list of initiatives and commits to a quarterly audit plan based on addressing the current high risks.

GETTING BUY-IN

Making changes to the way internal audit operates may not always be welcomed with open arms. In some

AUDITOR SPOTLIGHT

With 30 years of experience at D'Arcangelo & Co. LLP, an audit and consulting firm in New York State, Fred Lyons is an expert in the audit field. Here's what he shared with CaseWare Analytics during a recent interview.

Q: What is the most important process an audit team needs in order to be successful?

A: I think it's most important to establish a repeatable routine to gain an understanding of the data and identify potential risks. Consistently applying the same techniques to the entire population makes each audit more efficient and thorough.

Q: What are some key strategies your team follows?

A: The first is to always ensure that the data is complete and accurate. If the data is wrong, your conclusions will be wrong. When you receive a data file, validate it by looking at the control totals, date cut-offs, etc. You can also use the Field Statistics feature in a data analysis tool. Validating the data file is a habit you have to get into and that all new auditors need to adopt.

I also think it's important to not be tempted to only drill down into data where you expect to see results. Look at the data holistically so you can understand it and maybe find something unexpected. If we only chase our expectations, we won't find anything unusual.

Q: Can you give an example of a time you found something unexpected in the data?

A: Definitely. When we first started learning how to use IDEA, we found a $10 million difference between the total printed on the report and the data supporting it. That was just the tip of the iceberg! The finding prompted an investigation that later uncovered a fraud scheme. Discovering the unmatched data was key to exposing the fraud.

Q: Why do you use data analysis software?

A: Data analysis tools offer repeatable routines that help create efficiencies. IDEA is logically structured, easy to learn and it widens our coverage because we can analyze the entire data population.

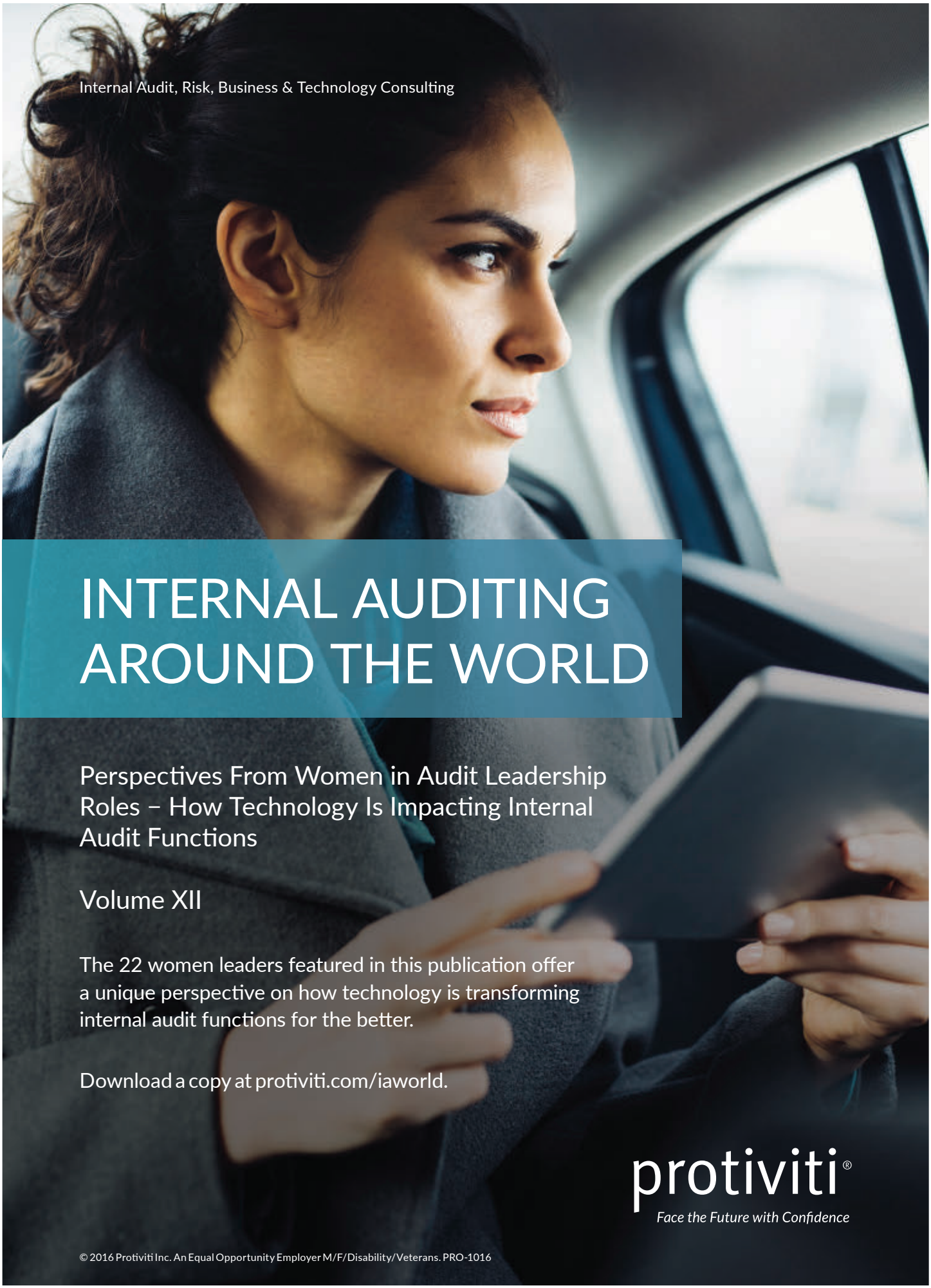
Another reason we use data analysis software is that it makes it easy for us to test and adjust our hypotheses when developing an audit routine. The fact that the source data is not altered is essential for us.

Q: Would you recommend IDEA?

A: Absolutely. It lets us quickly analyze 100% of our data using repeatable procedures. It's also advanced enough to provide what I call a 'one-click' solution where it creates a dashboard populated with charts and field statistics that make it easy to see the outliers. Generating a result with just a couple of clicks is awesome.

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

CaseWare ANALYTICS



Strategic **business risks** comprised only **8 percent** of CAEs' internal audit plans in 2016, according to The IIA's 2016 North American Pulse of Internal Audit report.

organizations or industries, long-established cultures and beliefs may not lend themselves to change—at least, not easily or quickly. If traditional internal auditing is the organization's expectation, the audit department must continue to perform it as effectively as possible, making sure to contribute value and communicate that value regularly (see "Making a Case for a More Strategic Approach" on page 25).

Lee says she believes in letting the work speak for itself. "Management appreciates receiving relevant and timely information," she explains. "If internal audit can provide information that will help executives do their job better or help them achieve their goals, then buy-in isn't a problem because they see value in internal audit's work."

But what if it is internal audit's own leadership that needs to be convinced of the value of a more strategic approach to internal auditing? According to Ames, "It's difficult for audit departments to break through from a routine, traditional approach to a more optimized, innovative view without support from the leadership in the audit department, itself. You might have a few who reach those levels, but never the whole department. And internal audit won't become a partner in the strategy."

The CAE is the linchpin. When risk is discussed in the organization, the CAE must step up to highlight the need for a strategic approach and explain the audit committee's mission. If the mission described in that explanation is focused only on protecting, the opportunities for enhancement may be limited. The opportunities are even more limited if the CAE chooses not to listen to his or her internal auditors' suggestions for how they can contribute more value to the organization. "Then perhaps it is time for the CAE to move on to another position," Hjelm suggests, while also admitting, "This is, of course, easy to say, but hard to do."

A VALUE-PRODUCING PROPOSITION

Regardless of where in the organizational chart minds need to be changed, those internal auditors who understand that expanding their efforts across the organization's value chain can help the department deliver increased risk coverage, cost savings, and measurable value to the business must carry the flag. And, in fact, that advocacy can play a key role in reaching the career goal many internal auditors set for themselves: becoming a trusted advisor. Hjelm explains that when risk turns to value, assurance also transforms to insight—a transformation expected of a trusted advisor. She counsels, "The audit report is not the main result of our work. The main result becomes our identification and description of what consequence a risk or a combination of risks has. Internal auditors' understanding, knowledge, and ability to communicate in business language can help the board and C-suite focus on 'hot' areas."

Focusing internal audit's activity on the strategic objectives that matter most to the organization is a value-producing proposition. And, in fact, while it is a topic of attention now, it may not be an entirely new concept. Perhaps it is, instead, a matter of recommitting to basic, long-held beliefs that may have slipped out of view for a time, in the rush of checking items off the daily to-do list. Baker notes, "We sometimes forget that our whole life in internal audit has involved objectives, risk, and controls. Sometimes we focus more on controls, other times we zero in on risk. But objectives have always been there. And if we don't assess risk and controls with objectives in mind, why do it?"

"If internal audit can provide information that will help executives do their job better or help them achieve their goals, then buy-in isn't a problem."

Lisa Lee

"If we don't assess risk and controls with objectives in mind, why do it?"

Larry Baker

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

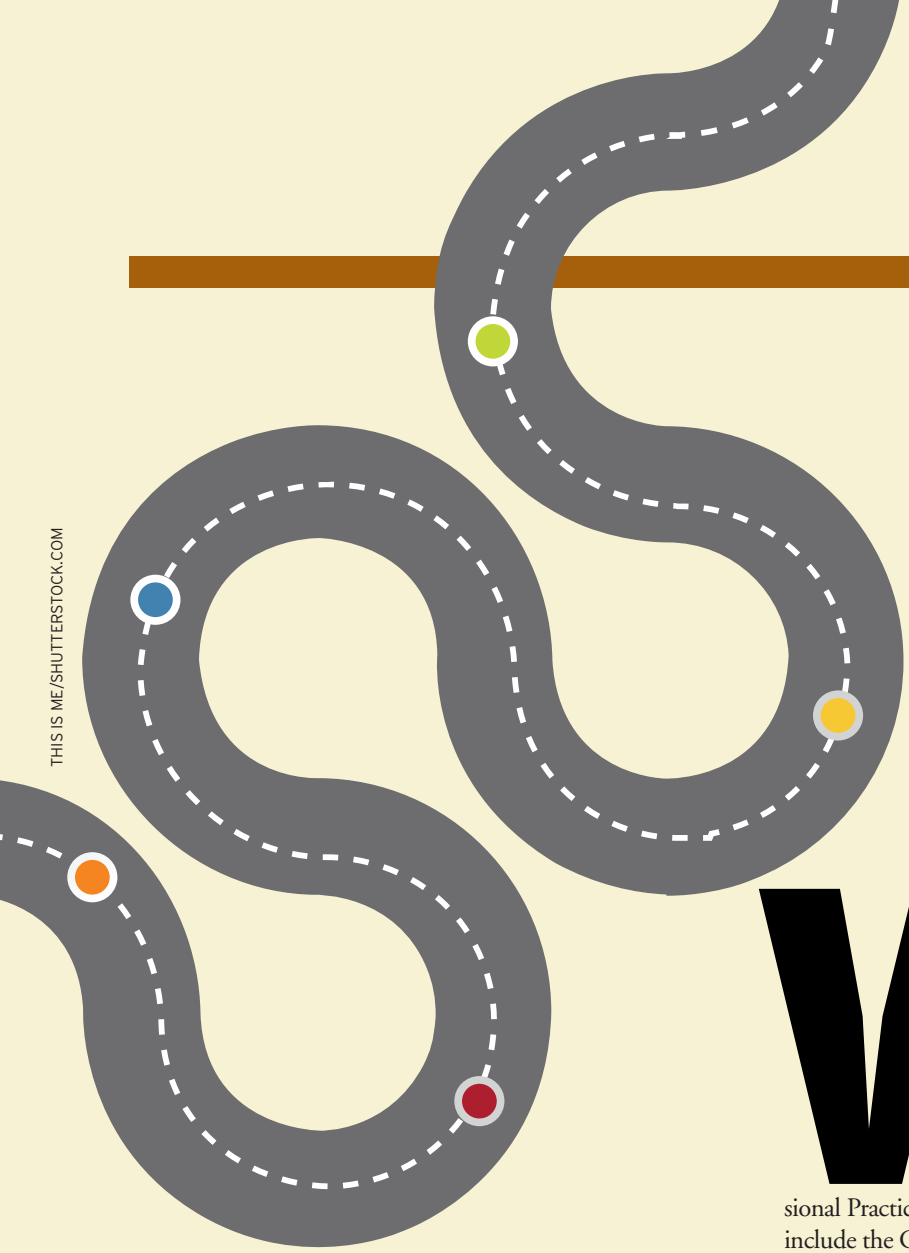
Internal Auditor magazine wants to help with your education.

We are offering six US$1,000 scholarships throughout the year to undergraduate and graduate students around the world. Download the scholarship application and apply today at **www.InternalAuditor.org/Scholarships**

75TH ANNIVERSARY 1941-2016

The Institute of Internal Auditors

2016-0443



THIS IS ME/SHUTTERSTOCK.COM

Core Principles and the QAIP

Demonstrating the effectiveness of the IPPF's Principles shows internal audit's alignment with stakeholder expectations.

Basil Woller

When the International Professional Practices Framework (IPPF) was updated in 2015 to include the Core Principles for the Professional Practice of Internal Auditing, it provided a significant opportunity to integrate and align these Principles into an internal audit activity's quality assurance and improvement program (QAIP). The challenge is how to do it in a practical and meaningful way that provides incremental value to the internal audit activity and its stakeholders. This is especially relevant in today's dynamic business environment, because demonstrating the effectiveness of Core Principles as a component of the QAIP supports the credibility and value of internal audit and promotes its role within the organization's governance structure.

The best way to integrate Core Principles into the internal audit activity's understanding of quality is to develop a concept and approach that is easy to understand, is adaptable to an individual organization, and provides insight into how effectively the Core Principles are being achieved. It also is important to understand how achieving Core Principles could be an integral component of the QAIP and an extension of the assessment process. Even though QAIP external assessments do not require auditors to evaluate conformance with the Core Principles, they are a mandatory element of the IPPF. As such, chief audit executives (CAEs) should have a perspective as to whether they are being achieved and a way to communicate that perspective

to key stakeholders in a way that is easy to understand and can be monitored, measured, and reported over time.

WHY INTEGRATE THE CORE PRINCIPLES?

Standard 1300: Quality Assurance and Improvement Program is designed to promote and support quality and continuous improvement in an internal audit activity. Internal and external assessment components provide a framework to ensure quality is embedded into internal audit processes and infrastructure. Communication of results to senior management and the board supports their fiduciary oversight of the internal audit activity. Achieving these Core Principles is a professional requirement. Embedding them into the QAIP is an effective way to ensure the internal audit activity is aligned with these mandatory IPPF elements or ensure that governance and oversight activities related to internal audit are consistent with successful practices and professional requirements.

HOW TO INTEGRATE THE PRINCIPLES

Quality standards require an evaluation of conformance with the Code of Ethics and the *International Standards for the Professional Practice of Internal Auditing*. It is assumed that if an internal audit activity is in general conformance with the Code of Ethics and the *Standards*, then it is achieving the Core Principles. As a result, even though Core Principles are mandatory, there is no mechanism defined to provide a CAE with a view toward whether the Core Principles are being achieved.

In fact, there are other characteristics that demonstrate whether an internal audit activity is achieving the Core Principles beyond conformance with other mandatory elements of the IPPF. The most appropriate mechanism to integrate Core Principles into the QAIP is to use a maturity framework to describe levels of maturity related to each principle. This can provide insight into achieving Core Principles efficiently using a combination of quantitative and qualitative characteristics to define maturity.

The QAIP provides quantitative characteristics to the maturity framework through its internal and external assessment requirements. Other qualitative characteristics that help describe placement on the maturity spectrum supplement the QAIP quantitative view. There are five steps that provide a roadmap for implementing a Core Principles Effectiveness Framework into a QAIP.

1 Establish a Maturity Framework

The Core Principles Effectiveness Framework (see "Core Principles Effectiveness Model" on this page) describes the infrastructure, process, and quality associated with differing levels of achieving effectiveness for the Core Principles. Progression along the maturity spectrum is a function of demonstrating characteristics associated with each level. Movement to a higher level of maturity assumes characteristics of all previous levels of maturity continue to be demonstrated. Placement on the maturity spectrum is a matter of professional judgment considering the "best fit" based on defined characteristics. Effectiveness progresses from:

1. **An ineffective level** – Infrastructure and processes supporting the internal audit activity are not well defined or operating effectively and there are many areas of partial or nonconformance with associated standards.

CORE PRINCIPLES EFFECTIVENESS MODEL

Core Principles for the Professional Practice of Internal Auditing	Not Effective	Partially Effective	Effective	Sustainable	World Class
Demonstrates integrity			•		
Demonstrates competence and due professional care			•		
Is objective and free from undue influence (independent)			•		
Aligns with strategic objectives and risks of the organization			•		
Is appropriately positioned and adequately resourced			•		
Demonstrates quality and continuous improvement			•		
Communicates effectively			•		
Provides risk-based assurance			•		
Is insightful, proactive, and future-focused			•		
Promotes organizational improvement			•		

Globally, just 37% of organizations are in conformance with Standard 1300, notes The Internal Audit Foundation's Internal Audit Quality Assurance and Improvement: A Call to Action report.

NOTBAD/SHUTTERSTOCK.COM

2. **A partially effective level** – Infrastructure and processes supporting the internal audit activity are defined and operating effectively but there are areas of partial conformance within associated standards.
3. **An effective level** – Infrastructure and processes supporting the internal audit activity are mature and there is general conformance with all associated standards.
4. **A sustainable level** – Quality programs are focused on continuous improvement and general conformance with associated standards is demonstrated for at least two consecutive external assessments.
5. **World class** – There is a drive and passion for continuous improvement using benchmark data and peer input, with external quality assessment taking place more frequently than once every five years with a focus on generating ideas for improvement.

Most organizations strive to be at an effective to sustainable level, as there are incremental costs associated with operating at a world-class level.

2 Map Core Principles With the *Standards* and Code of Ethics

Linking the Core Principles to associated professional guidance is the next critical step in the process. Without clear linkage, results of the QAIP, including internal and external assessment, cannot provide data for placement on the maturity spectrum. While linkage is subject to professional judgment, there are clear associations between the Core Principles and the Principles and Rules of Conduct in the Code of Ethics and the *Standards*. An example of linkage related to the Core Principle "demonstrates integrity" is shown in "Core Principles Mapping" on this page). This same linkage exercise needs to be conducted for all other Core Principles.

CORE PRINCIPLES MAPPING

Core Principle	Associated Professional Guidance	Rationale
Demonstrates integrity	Code of Ethics	The principle rule of conduct for integrity states, "The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment."
	Standard 1000	Establishes the foundational expectation that work will be performed in a manner consistent with the Code of Ethics.
	Standard 1100	Establishes the requirement that all work be performed in an independent and objective manner with disclosure of impairment.
	Other Standards	Each standard must be evaluated to identify and describe linkage.

3 Define Characteristics of Maturity

Placement of a Core Principle onto the maturity spectrum requires that characteristics specific to that level of maturity be defined. There are three aspects to characteristics that should be defined for each level. *Standards* and QAIP characteristics define maturity in terms of level of conformance with the *Standards* and the extent to which conformance is validated through internal periodic assessment or external assessment elements of the QAIP. Infrastructure and process characteristics define maturity in terms of level of formality and sophistication within the internal audit activity. These characteristics also attempt to describe behaviors within the internal audit activity that support differing levels of maturity. The third category comprises those characteristics specific to a Core

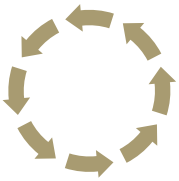
TO COMMENT on this article, EMAIL the author at basil.woller@theiia.org

Principle and might include examples of infrastructure, process, conformance, or successful practices that are unique to that Core Principle. Characteristics build upon those described for the previous level of maturity and should provide a clear view and differentiation between the levels. When viewed in combination, these definitions provide a useful tool to facilitate the placement of a specific Core Principle onto the maturity spectrum. As with any maturity framework, placement on the spectrum is a "best fit" based on the judgment of the professional performing the assessment. "Demonstrates Integrity Characteristics," this page, establishes the characteristics for the Core Principle, "demonstrates integrity." The *Standards*, QAIP, infrastructure, and process characteristics are the same for all Core Principles.

4 Perform Internal and External Assessment Consistent With Requirements of a QAIP

Evaluating the effectiveness of the Core Principles can only be accomplished when the results of the QAIP support placement of effectiveness within the maturity spectrum. A well-designed QAIP that includes internal and external assessment components and communication of those results provides the perfect platform for evaluation, placement, and communication of effectiveness. Ongoing monitoring of internal audit activity performance supports quality on an audit-by-audit basis. This is often supported by the definition, tracking, and reporting of key performance indicators (KPIs). The best way to monitor effectiveness is to identify Core Principles effectiveness as a KPI and report statuses related to maturity annually to senior management and the board. This further supports the board's fiduciary oversight responsibility of internal audit by providing insight into current and changing maturity levels for the Core Principles. Periodic internal

DEMONSTRATES INTEGRITY CHARACTERISTICS

Maturity Level	Standards and QAIP Characteristics
World Class 	» Generally in conformance with all associated standards. » External assessments performed more frequently than the five-year requirement.
Sustainable 	» Generally in conformance with all standards associated with the Core Principles. » Conformance demonstrated in at least two consecutive external assessments. » At least two consecutive external assessments performed. All external assessments performed within the five-year requirement.
Effective 	» Generally in conformance with all associated standards. » Internal assessments performed annually. » External assessment performed within the five-year requirement.
Partially Effective 	» Partially in conformance with an associated standard. » Generally in conformance with all other associated standards. » Internal assessments performed but not annually. » External assessment performed outside the five-year requirement.
Not Effective 	» Not in conformance with associated standards. » Partially in conformance with several associated standards. » Internal assessments not performed. » External assessment not performed.

REDKOALA/SHUTTERSTOCK.COM

29% of CAEs say their Quality Assurance and Improvement Program is nonexistent or ad hoc, according to the Internal Audit Quality Assurance and Improvement: A Call to Action report.

Infrastructure and Process Characteristics	Core Principle Specific Characteristics
» Internal audit charter supports internal audit role in Three Lines of Defense Framework. » Functional reporting to the board supported by active oversight processes. Administrative reporting includes seat at the table for executive-level strategy-setting and direction. » QAIP viewed as opportunity to become world class. Passion for excellence. Status quo not acceptable. » Active benchmarking with peers to identify ideas and opportunities for improvement.	» Independence and objectivity are supported by annual awareness training. » Independence and objectivity actively managed at individual, engagement, and internal audit activity level.
» Internal audit charter approved by the audit committee annually. » Functional reporting to the board and administrative reporting to the CEO. » QAIP in place with primary focus on continuous improvement. » Internal audit manual updated annually to ensure alignment with changes to the *Standards* and successful internal audit practice.	» Independence and objectivity are actively managed by internal audit. » Internal audit management and staff sign annual confirmation of independence and objectivity and agree to abide by the Code of Ethics.
» Internal audit charter approved by the audit committee. All required elements in place. » Functional reporting to the board and administrative reporting to a direct report of the CEO. » QAIP in place and documented with all required elements. » Internal audit infrastructure and processes defined and documented in manual. All required elements included.	» Internal audit charter requires conformance with the Code of Ethics. » Internal audit policies and procedures require conformance with the Code of Ethics. » Real or perceived conflicts of interest disclosed appropriately.
» Internal audit charter approved by the audit committee. Not all required elements in place. » Functional reporting to the board. Administrative reporting to level below a direct report of the CEO. » QAIP in place and documented but does not include all required elements. » Internal audit infrastructure and processes defined and documented in manual. Not all elements included.	» Internal audit charter references the Code of Ethics. » Internal audit policies and procedures reference the Code of Ethics.
» Internal audit charter not in place or not approved by the audit committee. » Functional and administrative reporting does not support independence and objectivity. » No QAIP in place. » Internal audit infrastructure and process not defined and documented in manual.	» Specific examples of operating in conflict with the Code of Ethics. » No disclosure of real or perceived conflicts of interest.

Certified Internal Auditor® | CCSA® | CFSA® | CGAP® | CPEA® | CPSA® | CRMA® | QIAL®

Drive Your Career Forward

IIA Certifications and Qualifications

An IIA Professional Credential can take your career in the right direction, whether you're just starting down the audit path or taking your career to new elevations. Drive to new opportunity, with increased earning potential*, deeper knowledge, and enhanced credibility.

*According to The IIA's 2017 Internal Audit Compensation Study, 51% of certified internal auditors have higher salaries than those who have no certification (based on U.S. responses).

Invest In Your Tomorrow, Today.
www.theiia.org/Certification

The Institute of Internal Auditors

2017-1636

assessment provides the opportunity to assess conformance with the Code of Ethics and the *Standards* to provide data associated with the defined characteristics, and is essential to provide insight into conformance in the periods between external assessments. An external assessment provides the perspective of an independent assessor or assessment team qualified in the practice of internal audit and external assessment related to levels of conformance. Frequency of external assessment is a factor in determining level of maturity.

5 Evaluate and Report Maturity Levels for Core Principles

Placement of maturity in the Core Principles Effectiveness Framework is a matter of professional judgment. Using a systematic and defined framework increases the likelihood that placement is appropriate and consistent with defined characteristics. A maturity framework provides the foundation and perspective to make reasoned and professional judgments regarding the levels of maturity for each Core Principle. From an organizational perspective, some principles might be more relevant than others in achieving objectives. Increasing the level of maturity and the resulting investment might be appropriate.

ALIGNING INTERNAL AUDIT

The Core Principles established in the IPPF describe the essence of an internal audit activity. Incorporating an evaluation of Core Principles into the QAIP provides the perfect mechanism to demonstrate to stakeholders that this mandatory element of the IPPF is relevant to the practice of internal auditing in the organization and that the internal audit activity is aligned to their requirements. Using a maturity framework provides a context for this communication that is measureable and easy to understand. It also provides better insight into the activities that support the profession and can promote a deeper understanding of internal audit's role in the governance mechanism of organizations. As the *Standards* change, the Core Principle Effectiveness Framework is scalable and adaptable. Each Core Principle's defined characteristics can be adapted to organizations and modified over time as circumstances warrant.

BASIL WOLLER, CIA, CRMA, *is principal and owner of Basil Woller & Associates in The Woodlands, Texas.*

BOOK EXCERPT By modeling high standards of ethical behavior, internal auditors can help shore up faith in the organizations they serve.

Champions of Trust

By Richard F. Chambers

Illustration by Timothy Cook

Public trust in government and big business is dropping at an alarming rate. Whether viewed through a political lens in the surprising Brexit and U.S. presidential votes, or the consumer and regulatory backlash against a corporation embroiled in scandal, the repercussions of those misgivings can be profound.

This growing distrust reflects a fundamental erosion of faith in the institutions that are the bedrock of modern civilizations. As internal auditors, we are guardians of trust in the organizations we serve, and to be effective, our stakeholders must be confident that we will do the right thing, speak the truth, and be courageous. I gave a great deal of thought to what makes a trusted leader while researching my new book, *Trusted Advisors: Key Attributes of Outstanding Internal Auditors*. My research, assisted by The IIA's Audit Executive Center (AEC), included surveying some of the top professionals in internal auditing about what attributes they believe are essential to becoming a trusted advisor. Toward the top of the list is ethical commitment. An excerpt from the book focuses on this trait and discusses why internal auditors must go beyond commitment and demonstrate ethical resilience.

I enjoy watching football (that is, American football, not soccer). Sometimes during the game, when an infraction is committed before the play begins, the referee will throw a penalty flag. The flag often signifies a false start if certain players on the offensive team move before they're supposed to. At times, there are referees who either ignore the infraction or are passive about making the judgment call.

Internal auditors who sit on the sidelines and fail to call out inefficiency, waste, fraud, or mismanagement are spectators. More commonly, internal auditors are referees, observing the plays that make up the normal course of business operations and blowing a whistle or throwing a yellow flag when circumstances warrant. They are objective in assessing whether a foul or infraction has occurred, but they are in reactive mode—responding to what took place in the past.

The most effective internal auditors are those with enough fortitude to blow the whistle before trouble ensues. They see troubling issues in the formation stage, raise a concern, and take a stand to ensure things are done right.

But, as I discovered years ago, there has to be a high degree of trust between internal auditors and those whom they are cautioning about pending wrongdoing or calamity. Without trust as a basis for engagement, the conversation can become awkward or even polarizing.

Ethics is an area that plays a significant role in my view of outstanding internal audit performance; so much so that I decided to feature ethical resilience as my first area of focus. I've been known to characterize ethics as "table stakes" for those wishing to engage in internal auditing. It's a strong statement, but I stand by it. Internal auditors can't accomplish their mission without a diligent, unceasing commitment to ethical behavior.

Larry Sawyer, an iconic internal audit author, wrote about the importance of trust in ethical behavior. He wrote, the "key to any profession is the trust placed in it by its clients." Everyone knows how important ethics are; that's a foregone conclusion. But I believe that, for internal auditors, ethical behavior is so critical, it goes beyond just a commitment. Outstanding internal auditors do more than just commit to ethics; they model ethical conduct in everything they do by being resilient, even when it may not be a popular stance. They may be tested ethically, but they withstand the challenges to their ethical convictions and bounce back stronger than ever.

Obviously, the CAEs who responded to the AEC survey agreed with this view. More than half of them selected ethical commitment as one of the top three traits shared by successful internal auditors.

Outstanding internal auditors do more than just commit to ethics; they model ethical conduct in everything they do.

Reinforcing that viewpoint, the Internal Audit Foundation's Common Body of Knowledge (CBOK) 2015 Global Internal Audit Practitioner Survey asked CAEs around the world to rate themselves on their perceived level of competency on 10 core competencies, with 1 being "novice" to 5 being "expert." The survey data indicated that CAEs rated themselves highest in ethics (4.3 overall), which validates my point that ethical resilience is a top attribute for outstanding internal auditors.

Paul Sobel, vice president/CAE for Georgia-Pacific LLC, states it very simply and powerfully: "In our role as auditors, ethics and integrity are the foundation for our ability to provide objective assurance, advice, and insights. In essence, it's the foundation for our credibility."

• • •

COMMITTING TO ETHICS

As the leader of a global organization that requires compliance with a formal Code of Ethics to serve as a member or hold a certification, I have an unwavering commitment to behaving ethically. At The IIA, we don't skirt the issue; we believe internal auditors must stand for what is right, adhere to the highest ethical code, and never yield to pressures to bend the rules. An ethical lapse by one internal auditor can

To hear Richard Chambers discuss attributes of outstanding internal auditors, attend the IIA members-only Trusted Advisors webinar on March 28 – visit www.theiia.org/key-attributes for details.

undermine trust not only in that individual but also in those around him or her. The higher in the organizational chart the transgression occurs, the more damaging the potential impact. We in the profession must share a commitment to ethics. For the most part, I believe we do.

In most organizations, the internal auditors are perceived as being far more likely to disclose ethical misconduct than to act unethically themselves. But we are human. I will never forget my surprise and disappointment when I viewed the results of a survey of 70 CAEs attending an IIA event a few years ago. One-third of the respondents acknowledged that they had "discovered or witnessed unethical actions" within their own internal audit functions.

Making the effort to clean our own ethical house is important not only in the context of what internal auditors do in their everyday jobs, but also in their role as business leaders. In her book, *7 Lenses: Learning the Principles and Practices of Ethical Leadership*, Linda Fisher Thornton says getting employees to act ethically is largely driven by their desire to "follow the leader." If they see top management behaving ethically, desiring to serve others, and making a positive difference, they are inclined to respond in kind.

Organizational commitment to ethical behavior is not just a matter of hosting an "ethics day" or showing a slide presentation during new-hire orientation, although all efforts at communicating expectations relative to ethics are valuable. The most impactful things leaders can do to influence employees are subtler: openly discussing ethical gray areas, acknowledging the complexities that can arise in work situations, treating ethics as an engrained way of behaving, celebrating displays of ethical conduct, showing respect for those with different opinions and difficult personalities, and expecting everyone to meet ethical standards.

These behaviors (at any rank in the organizational chart) should not be difficult. If we think of ethics as a way we interact, collaborate, and create synergies with others, it should be natural to act ethically and expect the same behavior from others.

An ethical lapse by one internal auditor can undermine trust not only in that individual but in those around him or her.

The results of such behavior can yield unexpected results. Early in my career as a CAE, the chief financial officer (CFO) asked my internal audit team to perform an audit. He had a strong personality and was sure the company was being billed for purchases it didn't make. He wanted my team to find evidence to support his belief. I sent the internal auditors to conduct the audit and they found no evidence of transgression, which put me in a bit of a tight situation. The support from the CFO and other executives was important and necessary to me, yet I knew that our audit results weren't what he wanted to hear. By telling him he was wrong, I risked losing both his fledgling trust in the internal audit department and his willingness to use us for future projects, but I knew I had to be straightforward with him. As expected, he did express some disappointment that we didn't validate his concerns.

Not long after that, he called me to ask my team to do some work in another of his functional areas. After I expressed our willingness to do so, I told him I was surprised he had contacted me for an additional project since I didn't give him the news he wanted to hear the last time. He responded that my honesty in those circumstances proved to him that my team and I would be fair and objective and he could rely on our work. I don't think he intended our first encounter to be a litmus test, but it was. Once your stakeholders have a chance to check your ethical compass and confirm that it's pointing true north, they know they can follow you because you won't lead them in the wrong direction.

ETHICAL BEHAVIORS

No one is saying that exercising ethical behavior is easy, but maybe half the challenge is in agreeing on exactly what constitutes ethical resilience. In the AEC survey, we used the following terms to elaborate on what we meant by ethical commitment, and I suspect few would argue with their inclusion:

- Integrity—being known for strict adherence to high moral principles.
- Courage—being brave enough, even in the face of professional or personal danger, to do the right thing.
- Honesty—displaying unwavering commitment to dealing in truth.
- Accountability—taking responsibility for our actions and the resulting perceptions.
- Trustworthiness—building a history of ethical behavior that forms a foundation upon which people can place their trust.

Courage especially seems to be a factor in ethical behavior. A number of the survey respondents ruminated on the importance of courage. Take the following comments, for example:

> *"Inner courage: to follow leads, to follow your gut belief, to professionally confront management and the board, to raise the questions few people want you to raise, to put it all on the line (in terms of taking the risk to do what is right)."*

> *"Courage: the ability to express one's opinion and give advice even when the ideas are not popular or wanted."*

> *"Courage to stand alone, if needed, when tough issues need to be raised to management and the board."*

VISIT our Mobile app + InternalAuditor.org to watch a video discussion on auditing the organization's ethical standards.

Courage is what drove Bethmara Kessler, senior vice president, integrated global services, and former CAE of Campbell Soup Co., to select ethical commitment as one of her top two choices in the AEC survey. She explains that courage is a particular challenge for auditors because in her long experience of managing audit teams, she has seen internal auditors sometimes waver in their defense of difficult findings for a variety of reasons: They, like most humans, want to be liked; they want to avoid difficult conversations; they feel the pressure to serve too many masters with competing needs; and they fear their actions may hinder their future career opportunities in the business. But, she remarks, "We have to remind internal auditors that courage is important and they should step forward when they see something. Look at Harry Markopolos, who tried multiple times to break open the Madoff scandal. He just kept going back to the [U.S. Securities and Exchange Commission] over and over to make his point. I'm sure it was not an easy thing to do. It took a lot of courage. In my view, he's a hero."

Another internal audit hero who deserves notice is Heidi Lloce-Mendoza, currently undersecretary general for the United Nations Office of Internal Oversight Services, and before that, commissioner and officer-in-charge of the Commission on Audit (COA) of the Philippines. Mendoza came to the world's attention as a result of a 2002 audit her team conducted that uncovered massive bid rigging by former Makati City Mayor Elenita Binay. Mendoza served as a government witness in some of the antigraft cases filed against the former mayor. In response to her speaking out against the former mayor's corruption, Mendoza's home was broken into multiple times and she was the target of threats that required special security protection. Yet, despite her admission that she was still being harassed about her role in the corruption trials 13 years after the fact, when she resigned from the COA in 2015 she indicated that her passion for her work had not abated and she felt "no pain, no trace of regret" for her experiences.

• • •

Ethical resilience is a trait that not only provides value in and of itself, it also supports the other traits mentioned in this book. Having a firm grip on our own ethical beliefs clears away some of the clutter that can distract us from focusing on desired results. ia

RICHARD F. CHAMBERS, CIA, QIAL, CGAP, CCSA, CRMA, *is president and CEO of The IIA.*

Trusted Advisors: Key Attributes of Outstanding Internal Auditors is available at The IIA's Bookstore.

Infusing IT Auditing Into Engagements

A three-phase approach can enable internal audit to build its IT-related capabilities.

Andrew Bowman
Haylee Deniston

Modern technology is growing rapidly, as is the level of disruption driven by it. In the 2016 Technology Industry Outlook, Deloitte describes the technology sector reaching a tipping point "where cognitive computing, big data analytics, cloud computing, and the rapidly growing Internet of Things are transforming businesses around the globe—including those outside the technology sector."

Internal audit is being transformed, as well. As advancements in technology drive changes in business operations, internal audit must perform IT audits to help organizations accomplish new and evolving business objectives. That requires the internal audit department and individual auditors to develop IT-related capabilities that are aligned with business risk. Skills that were once considered specialties of IT auditors are now required of all internal auditors. Those practitioners who cannot incorporate

technology into their assurance and advisory work will not be able to keep up with the evolving risks, strategies, and needs of their organizations.

Like any new audit endeavor, internal audit needs to gather information and form a plan for incorporating IT audit techniques into their audit work. Although each organization will require a different mix of effort and materials to obtain this information, some common elements are needed to prepare a comprehensive plan over the short (2 to 3 years), middle (3 to 5 years), and long term (5 to 7 years). The timing in which internal audit implements these elements may vary based on the organization, internal audit department, and internal auditors' capabilities. At each stage, the elements should be completed concurrently, with the internal audit department thinking holistically about the future of integrated auditing at its organization.

SHORT TERM Core IT Audit Capabilities

A separate IT audit is not required to start infusing IT-related capabilities into the current internal audit function; already-scheduled audit engagements can incorporate elements of IT auditing, further enabling the internal audit department to identify resources and education needed in the long term. As the internal audit department becomes more knowledgeable about the organization's IT environment, auditors can educate organizational management about the benefits of IT auditing in relation to business objectives. In the short term, the department should focus on creating a solid foundation that allows for development of future efforts.

Incorporate IT Perspective Into Current Audit Engagements Internal audit management should encourage staff members to incorporate IT audit methods into their engagements. During the planning phase, auditors should recognize the role IT plays in the internal controls for the processes currently being audited. Document internal audit's understanding of the organization's IT environment. For example, when auditing the accounts payable process, auditors should not only interview the accounts payable clerk about internal controls, but also talk to the individuals responsible for maintaining and supporting accounts payable data and processing systems. Moreover, internal audit should document automated controls such as access controls to the vendor master file.

Locate and read IT policies, focusing on change management, segregation of duties, and information security. Consider obtaining training from IT experts on applications used within the organization such as enterprise resource planning (ERP) software. Areas in which internal audit should develop skills include cybersecurity, data mining, audit analytics, crisis management planning, vendor governance, corporate and data governance, continuous auditing, and software and system life cycle management.

Identify Resources Leveraging their knowledge of the organization's IT environment, internal auditors should inventory the IT resources used across the organization. Start with core functions, including resources driving financial, human resources, and customer data. IT resources include IT platforms (servers, routers, and workstations) and software (databases, and proprietary and off-the-shelf applications). In the accounts payable example, IT resources could include ERP software and other electronic records such as spreadsheets used to house important calculations.

Second, pinpoint data stored on these core IT resources that are vital to current operations and achieving key business objectives. Key data could include vendor bank account, address, and contact information, as well as invoice distribution coding. Analyze current risk assessments of the underlying risks of this data. Examples of accounts payable risks include phantom vendors, duplicate payments, and corrupt or incorrect data. Assessing the current landscape reveals the most critical IT systems and data that need to be audited. Map core IT resources and data to key business objectives.

Respond to IT Risks and Identify Audit Objectives That Can Add Value IT supports nearly all business functions and allows management to make accurate, timely, and appropriate decisions that drive business operations. Integrated audits can support management's risk assessment to help align business objectives and IT. Research by Peter Weill and Jeanne Ross, published in the *MIT Sloan Management Review*, shows that appropriate alignment of organizational objectives and IT can deliver as much as a 20 percent higher return on investment.

Internal audit should identify top areas for review, with estimated resource requirements, based on the risk assessment and the risk tolerance

47% of audit leaders say their department is slightly or not involved in evaluating the quality of data used in their organization, The IIA's 2016 North American Pulse of Internal Audit report notes.

MIDDLE TERM Advanced IT Audit Capabilities

While using the current audit engagement schedule in the short term, chief audit executives (CAEs) should evaluate the department's preparedness to grow into a more mature model in which individual IT audit engagements are expected and the CAE has worked with organizational management to link business risks with IT audit techniques. In the middle term, internal audit must get the right people on board and work with the IT department and the organization at large to use a common IT framework. Moreover, it should partner with management and the IT department to facilitate long-term planning.

Build a Team Audit leaders should recruit qualified personnel with IT skills within the internal audit department. Look for people within the department who have current IT audit skills or an aptitude for technology that would enable them to gain those skills. Create a training plan that will address the core IT systems used within the organization and IT audit areas that will need to be covered in future audits. Consider hiring an IT expert into the internal audit department to help the department establish a solid relationship with the IT department.

Understand the IT Framework Organizations perform optimally when they use a consistent IT framework, which requires assessing the current state of the IT environment, defining a target state, implementing improvements, operating and measuring, and monitoring and evaluating. Examples of frameworks and standards include the International Organization for Standardization's ISO/IEC IT standards, ISACA's COBIT, and the U.S. National Institute of Standards and Technology Cybersecurity Framework. If the organization has not implemented an IT framework, internal audit should highlight the need for one that will allow for communication across business functions. Use of an IT framework helps determine whether the organization's IT business objectives comply fully with business rules and are structured, maintainable, and upgradable.

Perform IT Audits Identify the scope of IT audits that can be handled internally based on the IT experience of internal auditors and outsource coverage of any remaining risks. Consider the organization's adoption of the IT framework and the amount of resources management has devoted to the endeavor. Specific areas audits should address include: 1) segregation of duties to ensure the integrity of automated controls; 2) security, including physical and logical access, to safeguard the core systems as well as critical and sensitive information; and 3) change management to ensure integrity of system changes. A benefit to implementing an IT framework is access to audit programs that are available for these three areas as well as additional auditable areas for future engagements. Internal auditors should devote time to understanding the audit programs and the areas they cover so they will obtain efficiencies.

Foster Relationships With IT and Management Internal audit's relationship with the IT department is the foundation of a successful IT audit engagement. Internal audit should understand the metrics and goals the IT department uses in the monitoring and evaluation process of the IT framework. Through this process, internal audit can determine whether the linkage of IT metrics and objectives aligns with organizational goals. Moreover, it can allow internal audit to help discover and articulate to organizational management which IT initiatives can produce cost savings. Additionally, understanding the IT department's goals and metrics can help internal audit facilitate communication between the IT department and management. The value provided from these efforts can position internal audit to recommend enhancements to achieve operational goals.

of the organization. For example, the business may have an objective to take advantage of potential vendor discounts by making timely payments. Related IT risks include inappropriate access to vendor data, delayed access to invoice information that hinders decision-making, and incorrect calculation of the cost/benefit of taking discounts. An integrated audit of accounts payable could leverage accessing and identifying critical information to meet the business objective.

The Essential Experience For CAEs

2017 GENERAL AUDIT MANAGEMENT CONFERENCE

March 20–22, 2017 / Gaylord Palms / Orlando, FL

Fostering Risk Resilience

Join us in beautiful Orlando for the premier experience for audit leaders to explore emerging issues. This year's agenda perfectly aligns with recent headlines and can help you establish proven security measures that abide by best practices for optimal results.

Earn up to 18.3 CPE credits as you gain real-world knowledge from expert practitioners who lead more than 50 general and concurrent sessions in the following tracks:

- Mitigating Risk in Information Technology
- Meeting Evolving Stakeholder Expectations
- Supporting Governance and Addressing Risk
- Delivering Innovation in Internal Audit
- Maximizing Talent and Resources
- In Conversation With…

Audit Executive Center® Pre-conference Forum & Networking Event*
Sunday, March 19
1:00 to 5:00 pm

For more information, contact cae@theiia.org.

*For Audit Executive Center members only.

Register now at www.theiia.org/GAM.

The Institute of Internal Auditors

2017-0085

26% of respondent organizations' audit methodologies are supported by technology, and 13% use technology extensively, according to the 2016 Internal Audit Common Body of Knowledge study.

Internal audit can take a measured approach to cultivate IT-related capabilities.

TO COMMENT on this article, EMAIL the authors at andrew.bowman@theiia.org

LONG TERM
Advanced and Emerging IT Audit Capabilities

As the department's IT audit capabilities solidify and mature, it is a good time to start thinking about the long-term direction in which they will be applied to audit engagements. Performing IT audit engagements should give the department the foundational knowledge needed to help its consulting efforts. In the long term, internal audit should continue to develop and mature integrated engagements, grow consulting engagements, and improve IT audit skills with a focus on how organizational IT objectives will shape internal audit.

Leverage Data Analysis Data analytics allow internal audit to search for patterns and plausible interrelationships and anomalies, helping improve operational efficiency and effectiveness, as well as fraud detection and prevention. Moreover, analytics can enable reliable financial reporting and adequate compliance with laws and regulations.

The best time for internal audit to perform data analysis is early in the IT life cycle, when it can enable auditors to use time and resources more effectively. In this way, using data analytics can better inform IT audit planning and foster a more dynamic internal audit environment that moves from a traditional and post-mortem planning strategy to one that is more innovative and consultative.

Obtain Professional Certifications IT audit techniques cannot reach their maximum potential without adequate training. One of the best ways to achieve this level of aptitude is by obtaining professional certifications that attest to the practitioner's knowledge of technology and internal audit. Working toward certification enables individuals to gain IT audit knowledge. Maintaining certifications also requires auditors to complete continuing education to meet changes in technology and their associated risks. The specific mix of professional certifications should relate to the organization's objectives and core IT systems and data. Good qualifications to start with include The IIA's Certified Internal Auditor designation and ISACA's Certified Information Systems Auditor and Certified in Risk and Information Systems Control certifications.

RISE TO THE OCCASION

Internal audit's need to establish its IT audit capabilities and apply them to all of its audit engagements is increasingly important, now that technology is tightly integrated into business processes. Technology is influencing both what is audited and the way audits are being performed. Internal audit departments need to develop the essential skills to audit IT-based controls and processes and to identify operational improvements throughout their organization. Internal audit can take a measured approach to cultivate IT-related capabilities over time in conjunction with organizational management. Ia

ANDREW BOWMAN, CPA, CISA, CFE, *is a senior internal auditor at Los Alamos National Laboratory in Los Alamos, N.M.*
HAYLEE DENISTON, CPA, *is a senior internal auditor at Los Alamos National Laboratory.*

With the right strategy, practitioners can divide conformance into bite-size, easily digested portions.

To some, the idea of tackling conformance with the *International Standards for the Professional Practice of Internal Auditing* may seem like a steep, uphill climb. The phrase "conformance with the *Standards*" can sound authoritative and overwhelming, suggesting a complex, resource-intensive effort. But conformance is actually much easier to achieve than many chief audit executives (CAEs) may think. In fact, numerous activities performed by practitioners likely conform with the *Standards* already.

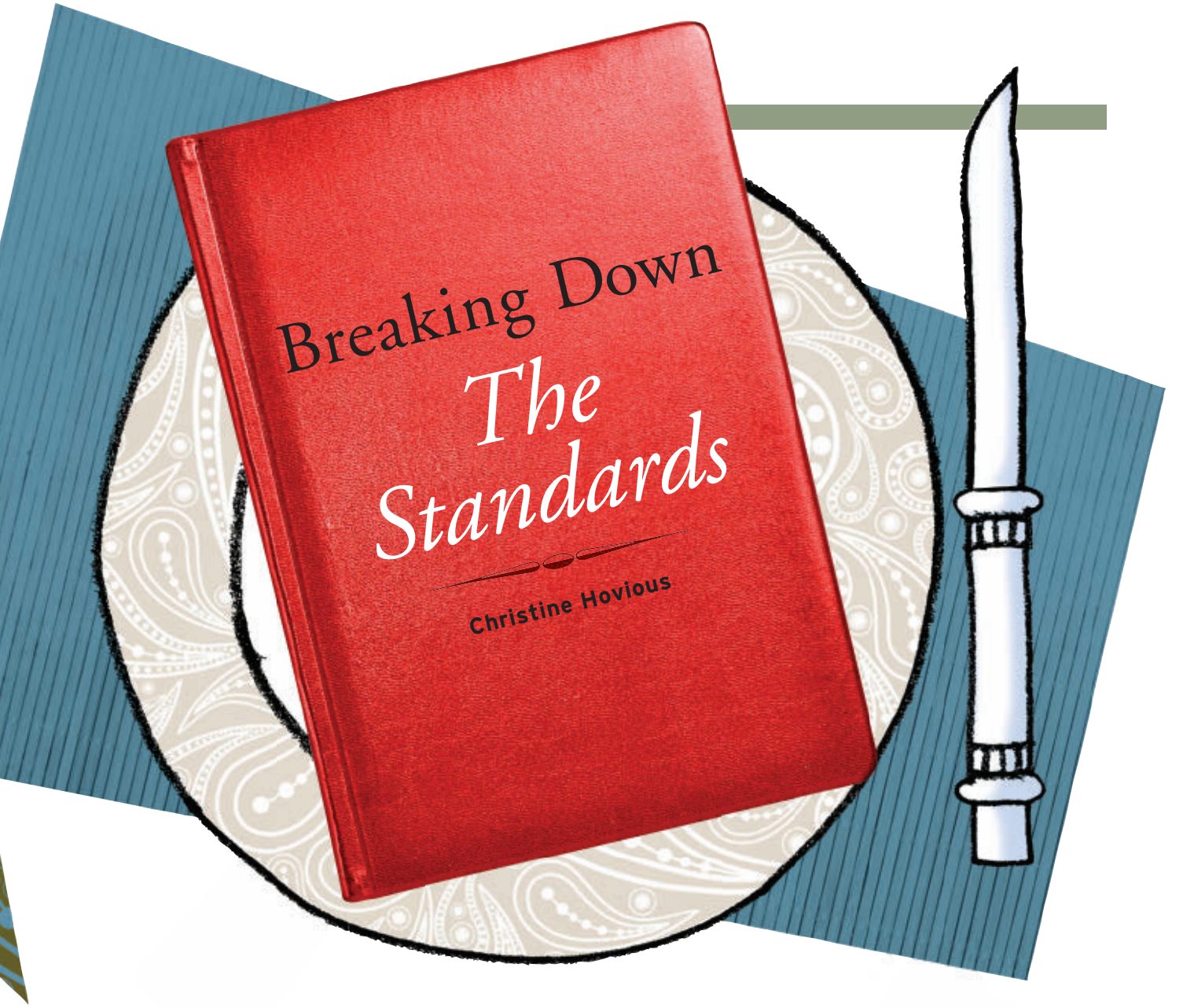
Composed of principles-based, core requirements, the *Standards* provide a framework for performing and promoting internal audit services and are essential in meeting the responsibilities of internal auditors and the internal audit activity. Conformance with The IIA's cornerstone of Mandatory Guidance begins with an awareness of the *Standards* and of how they provide a blueprint for the internal audit activity to evaluate and contribute to the improvement of organizational governance, risk management, and control processes. The *Standards* consist of two main categories:

- Attribute Standards (series 1000–1322) address the attributes of organizations and individuals performing internal auditing.
- Performance Standards (series 2000–2600) describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured.

A close examination of these areas reveals a relatively simple path to conformance, and one that many practitioners may already have begun to take. While not intended to provide confirmation of conformance, thinking about the *Standards* as advised can help internal auditors better navigate the requirements and streamline their approach.

ATTRIBUTE STANDARDS

Attribute Standards help establish the internal audit activity's position within the organization. Performance Standards, by contrast, involve the performance



IMAGES: PAISLEY: SHALDARK ILLUSTRATIONS; RED BOOK: ENSUPER; PLACEMAT TEXTURE: MEXRIX / SHUTTERSTOCK.COM

of internal audit responsibilities such as planning engagements, performing engagements, and communicating results. The majority of internal audit activities likely expend most of their effort focusing on Performance Standards, which may explain why some of the most common areas of nonconformance have fallen within the Attribute Standards (see "Top Areas of Nonconformance" on page 53).

Conformance with the Attribute Standards can be assessed by breaking them down into simple concepts: 1) reviewing the internal audit charter; 2) determining the independence of the internal audit activity and objectivity of the internal auditors; 3) evaluating the proficiency and due professional care with which engagements are performed; and 4) confirming the completion, maintenance, and communication of the quality assurance and improvement program (QAIP). "Attributes Standards Overview," on page 52, provides a detailed breakdown along each of these areas.

For existing internal audit activities, these concepts should already be established. Evidence of conformance can be demonstrated by ensuring that all elements

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

of the Attribute Standards are formally documented—or by reviewing existing documentation and updating it as necessary. Newly formed (or forming) internal audit activities should determine how they are going to apply the Attribute Standards, and then implement and document them, as they help set the stage for why the internal audit activity exists and how it will function.

The easiest way to determine the level at which an internal audit activity conforms with the *Standards* is through an internal assessment. QAIPs require an internal assessment, which, per Standard 1311: Internal Assessments, includes:

- Ongoing performance monitoring, using processes, tools, and information considered necessary to evaluate conformance with the Code of Ethics and the *Standards*.
- Periodic assessments to evaluate conformance with the Code of Ethics and the *Standards* performed by someone in internal audit or within the organization with sufficient knowledge of internal audit practices. The individual must possess at least an understanding of all elements of the International Professional Practices Framework (IPPF).

Such steps may already be incorporated into the routine policies and practices currently used to manage the internal audit activity. If the activity is already performing ongoing monitoring and periodic assessments as described, then it may be in conformance with Standard 1311.

The internal audit activity must also conduct an external assessment every five years, at minimum, to conform with the 1300 series. Ensuring this assessment is completed may demonstrate conformance with Standard 1312: External Assessments.

PERFORMANCE STANDARDS

Performance Standards consist of steps internal auditors perform on a regular basis. Four of the top 10 standards least conformed with, according to IIA Quality Assurance data, consisted of Performance Standards. As with the Attribute Standards, conformance with Performance Standards can also be broken down into simple concepts.

Standards series 2000 requires all internal audit activities to be managed effectively with policies and procedures to ensure value is added to the organization. The process includes establishing, communicating, and obtaining approval on a risk-based plan that can be deployed by appropriate and sufficient resources. Most internal audit activities likely follow these principles and therefore may conform to this series.

The 2100 series pertains to the nature of audit work and requires internal audit activities to evaluate and contribute to the improvement of the organization's governance, risk management, and control processes by using a systematic, disciplined, and risk-based approach. Conformance with this series of standards requires the internal audit activity to devise an appropriate strategy to evaluate the organization, which involves:

1. Obtaining an understanding of how the organization makes decisions, manages and communicates risk, promotes ethics and values, and ensures effective performance and accountability (Standard 2100: Governance).
2. Evaluating risk exposures and assessing the adequacy and

ATTRIBUTES STANDARDS OVERVIEW

1. Standard series 1000—the internal audit charter must:

- Formally define the purpose, authority, and responsibility of the internal audit activity consistent with the Mission of Internal Audit and recognize the mandatory elements of the International Professional Practices Framework (IPPF).
- Be documented, reviewed by the chief audit executive periodically, and approved by senior management and the board.
- Define the nature of assurance and consulting services.

2a. Standard series 1100—the internal audit activity must:

- Report to a level in the organization that allows the ability to fulfill its responsibilities in an unbiased manner.
- Determine the internal audit scope, perform work, and communicate results without interference, or it must disclose such interference and implications to the board.
- Confirm its organizational independence to the board, at least annually.
- Communicate and interact directly with senior management and the board with unrestricted access.
- Perform engagements without compromising quality or subordinating judgment on audit matters to others.
- Implement safeguards to limit impairments to independence or objectivity if asked to take on non-internal audit roles and responsibilities.
- Collectively possess or obtain the competencies required to

Nearly 25% of internal auditors rate themselves below competent in applying the IPPF to their work, according to the Looking to the Future for Internal Audit Standards CBOK report.

TOP AREAS OF NONCONFORMANCE

The IIA's Quality Services identified the top 10 standards least conformed with, in order, by organizations for which it had performed an external quality assessment in 2015. All Attribute Standards from the listing also appeared in the top 10 from 2014.

Rank	Attribute or Performance	Standard
1	A	**1311** Internal Assessments
2	A	**1010** Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter
3	A	**1320** Reporting on the Quality Assurance and Improvement Program
4	A	**1310** Requirements of the Quality Assurance and Improvement Program
5	A	**1312** External Assessments
6	P	**2020** Communication and Approval
7	P	**2300** Performing the Engagement
8	P	**2100** Nature of Work
9	P	**2500** Monitoring Progress
10	A	**1300** Quality Assurance and Improvement Program

perform its responsibilities or decline the engagement.

2b. Standard series 1100—internal auditors must:

- Be impartial, unbiased, and avoid situations involving competing professional or personal interest.
- Disclose to appropriate parties all instances in which independence or objectivity may in fact or appearance be impaired.
- Refrain from engagements in functions over which operations were performed, responsibility was held, or consulting services were provided that may cause a potential impairment.

3. Standard series 1200— internal auditors must:

- Possess the proficiency to perform their professional responsibilities effectively, including the ability to evaluate fraud risk and sufficient knowledge of key IT risks and controls.
- Exercise due professional care, consider the use of available tools and techniques, be alert to significant risks, and consider the needs, expectations, cost, complexity, and extent of work required to complete their engagements.
- Continue to enhance their knowledge, skills, and other competencies through professional development.

4. Standard series 1300—the quality assurance and improvement program must:

- Be developed, maintained, and include all aspects of the internal audit activity.
- Evaluate conformance with the *Standards* and application of the Code of Ethics.
- Include internal assessments (ongoing monitoring and periodic assessments) conducted by someone with sufficient knowledge of all elements of the IPPF.
- Include an external, qualified, independent assessment at least every five years.
- Communicate the results to senior management and the board.
- Contain results to support the use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*" (if the statement is used).
- Disclose nonconformance and the impact to the overall scope or operation of the internal audit activity to senior management and the board, if applicable.

More thorough assistance on conforming with the *Standards* can be found in the new Implementation Guides at www.theiia.org/ig

WORK PROGRAM

Internal assessments need not be complicated and can be as easy as creating a simple template. This example reflects a template to complete an assessment for IIA Standards 2240 and 2240.A1.

Standard	Process	Evidence	Status/ Gaps
2240: Engagement Work Program Internal auditors must develop and document work programs that achieve the engagement objectives.	An audit program is developed at the completion of the planning phase. The program includes the objectives and scope of the engagement, with detailed audit steps. The engagement work program contains key risks and controls under review, along with the resources available and proficiency of each.	Documented work program with evidence of approval, including date approved. Audit program was approved before commencement of fieldwork (see 2240.A1).	Generally Conforms
2240.A1 Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.	The work program contains detailed audit steps, including: » Audit techniques that will be used to identify, analyze, and evaluate information. » Nature, extent, and timing of audit steps. » Documentation requirements. The work program is reviewed and approved by the chief audit executive (or designee) before engagement commencement.	Work program was dated, contained review notes, and was signed before implementation (as evidenced per email communication and fieldwork start date). Confirmed that no adjustments were made to the work program by comparing the original work program submitted for approval to the final work program.	Generally Conforms

effectiveness of controls in responding to risks relating to governance, operations, and information systems regarding the achievement of strategic objectives, reliability and integrity of financial and operational information, effectiveness and efficiency of programs and operations, safeguarding of assets, and compliance with internal and external requirements. The evaluation should also include examining the potential for the occurrence of fraud and how fraud risk is managed (Standard 2120: Risk Management and Standard 2130: Control).

Performance Standards series 2200 through 2400 describe the audit engagement process. All internal audit activities should follow the basic engagement process, which consists of three parts:

- 2200 Series: Engagement Planning — determining objectives and scope, assessing timing considerations, and allocating resources to create and document a work program that considers the relevant strategies, objectives, and risks of the organization.
- 2300 Series: Performing the Engagement — conducting fieldwork, which includes identifying, analyzing, evaluating, and documenting appropriate information to support the engagement results, as well as supervising the engagement effectively.
- 2400 Series: Communicating Results — providing timely, quality results to the appropriate recipients that include the engagement's objectives,

Almost 20% of internal auditors say they fail to conform with The IIA's *Standards* because the process is too time consuming, according to Looking to the Future for Internal Audit Standards.

scope, results (applicable conclusions, recommendations, and/or action plans), and applicable disclosures.

Most internal audit activities likely conform to these standards in principle—in other words, they conform with the essence of the requirement.

Internal audit activities that maintain a monitoring process to follow up on the disposition of outstanding audit engagement results most likely also conform to Standard 2500: Monitoring Progress. Conformance can be evidenced by a routinely updated exception tracking system, which may be a spreadsheet, database, or other tool.

Lastly, Standard 2600: Communicating the Acceptance of Risks, requires the CAE to use judgment to determine whether management has accepted a level of risk that may be unacceptable to the organization. This standard obligates the CAE to attain an understanding of the organization's risk tolerance and risk acceptance process (if one exists). If the CAE concludes that an unacceptable level of risk has been accepted, the matter must be discussed with the organization's senior management; and if it is not resolved, the matter must be brought to the board's attention.

EASIER THAN IT SEEMS

Internal auditors need to remember that conformance does not hinge on following a set of prescribed rules. Instead, conformance is about understanding and achieving the principles behind the *Standards*. Demonstrating conformance is as simple as identifying current processes in place related to each standard and then documenting sufficient evidence (see "Work Program" on page 54 for an example of a straightforward assessment).

The effort does not have to be daunting or consume an inordinate amount of resources. By reading and understanding the IPPF, including the new Implementation Guides and related Supplemental Guidance, and documenting their work, practitioners can easily align themselves with professional standards and enhance their value to the organization. ia

CHRISTINE HOVIOUS *is director, Global Standards and Guidance, at The IIA.*

28TH ANNUAL ACFE GLOBAL FRAUD CONFERENCE

JUNE 18-23, 2017 / NASHVILLE / MUSIC CITY CENTER

From saving millions of dollars each year to mitigating reputational damage to their organizations, **FRAUD FIGHTERS LIKE YOU** are making an **IMPACT** around the world. More than 3,000 of these leading anti-fraud professionals will unite in Nashville to share insights and best practices.

WILL YOU BE AMONG THEM?

Keynote Speakers

Andrew Jennings
Investigative Reporter, First to Uncover Corruption Within FIFA

Eugene Soltes
Author, *Why They Do It: Inside the Mind of the White-Collar Criminal*

Eric O'Neill
Former FBI agent who helped capture Robert Hanssen, the most notorious spy in U.S. history

WHERE HEROES UNITE

Register by April 5 to **SAVE $200!**

FRAUDCONFERENCE.COM

Auditing Organizational Governance

Internal audit has an integral role to play in improving the organization's strategic performance.

Sridhar Ramamoorti, Alan N. Siegfried, and P. Alan White

Organizational governance is a broad concept that ensures superior strategy formulation, development, and execution in ways that balance performance, conformance, and accountability. It includes systems, controls, and associated processes that promote ethics and values, performance and accountability, and risk communication and coordination among the board, external and internal auditors, and management in meeting and exceeding stakeholder expectations. Internal audit's role in organizational governance has always been recognized and valued, but it has become increasingly important in the wake of governance failures in financial and public sectors throughout the world. As a result, more and more boards as well as executive management are turning to internal audit for assurance on governance effectiveness, culture, and strategy implementation.

The IIA's 2015 Global Internal Audit Common Body of Knowledge (CBOK) Practitioner Survey assesses the current role of internal audit in the governance process and how it can better position itself to contribute to effective organizational governance. Through their work, internal auditors can help achieve a balance between value creation (i.e., profitability and growth) and value preservation (i.e., sustainable, long-term performance). Governance reviews give internal audit the opportunity to help prevent governance failures and improve strategic performance. However, to take advantage of these

opportunities, internal audit must continue to embrace these assurance and advisory roles related to governance and adapt and evolve globally.

The survey's key findings include:

- Four out of 10 internal audit functions say a governance code is in place at their organization.
- About 27 percent say internal audit conducts extensive reviews of organizational governance.
- More than six out of 10 say their organization has a long-term strategic plan in place.
- Only 16 percent say internal audit conducts reviews of their organization's strategy.

The fact that less than one in five internal audit functions conduct extensive reviews of their organization's strategy is problematic, because it is impossible to provide assurance without fully understanding the organization's strategy. Specifically, in such a scenario, it becomes difficult to identify when executive management is pursuing riskier strategies at the expense of stockholders, or inappropriately placing a premium on short-term risk taking rather than long-term, sustainable value creation.

Culture can be a driver and enabler of effective governance and performance.

Corporate governance failures can be viewed through the prism of "information integrity," as executives and boards use information to make decisions. Information integrity failures can be traced back to information errors, ethical lapses, integrity failures, or a combination of these factors. Accordingly, governance audits and reviews primarily focus on validating the information used for strategic decision-making, or provide the context in which relevant information can be meaningfully interpreted.

THE GOVERNANCE AUDIT APPROACH

Assurance activities are intended to protect against governance failures, while advisory activities permit superior execution of strategy for growth, performance, and overall success. Both activities rely on a deep understanding of how organizational culture can be a driver and enabler of effective governance and superior performance.

Owing to political and cultural barriers within organizations, it may be difficult to have an audit plan approved with a separate comprehensive audit of governance. The chief audit executive (CAE) may be more successful using a strategy that incorporates governance reviews and recommendations as part of routine audits.

Using this approach, internal auditors address governance as a part of assurance or advisory services, rather than launching an enterprisewide governance audit or a comprehensive governance review. Conducting smaller, more digestible governance reviews during routine audits can serve to change attitudes from within the business organization and help lay the foundation for a subsequent comprehensive governance audit when the time is right.

Internal auditors in highly regulated organizations often find it easier to incorporate governance reviews into their audit universe, especially if the regulatory agencies express specific expectations for governance activities to be performed and monitored.

Governance audits must be based on two pillars:

1. Auditing governance structures and processes by providing assurance about information used for strategic decision-making (mostly based on hard controls where an analytical approach can be helpful).

On average, 57% of CAEs report that their board supports internal audit reviews of governance policies, according to The IIA's CBOK 2015 Global Internal Audit Practitioner Survey.

FOCUS ON RISKS

The board's focus is understandably on governance, while executive management's focus is more on enterprise performance. The CBOK survey asked internal audit practitioners what they thought about:

- Corporate governance risk (CGR) and strategic business risk (SBR), in terms of placing them in the top five risks for their organization.
- The audit committee's assessment of the importance of CGR and SBR in terms of being in the top five risks affecting their organization.
- Executive management's assessment of the importance of CGR and SBR in terms of being in the top five risks affecting their organization.

While internal audit and the audit committee have similar perceptions, especially in reference to corporate governance risk, executive management is least concerned about corporate governance risk (a value preservation orientation) and most concerned about strategic business/performance risk (a value creation orientation). Therefore, executive management exhibits the widest gap between perceptions of risk related to governance and performance as illustrated below.

? What are your organization's top 5 risks

	Corporate Governance Risk	Strategic Business Risk	Gap
Internal Audit	45%	55%	10%
Audit Committee	44%	63%	19%
Executive Management	36%	70%	34%

2. Auditing organizational culture where qualitative factors may need to be assessed and interpreted contextually to assess risk (mostly based on soft controls where intuition, common sense, and understanding of human behavior are indispensable).

GOVERNANCE STRUCTURES AND PROCESSES

Ensuring that an organization has a sound governance structure with effective and ethical policies and practices—along with decision-relevant information that is accurate, reliable, and timely—is critical to the organization's success. These combined factors, including a credible attitude of transparency and accountability, impact the company's reputation, stakeholder satisfaction, and overall growth and profitability. A wide swath of stakeholders, including the board of directors and executive management, seeks assurance about the information they use for strategic decision-making. They also need assurance that the organization's governance structures and processes, founded upon a well-established system of internal controls, operate effectively to achieve objectives, increase company profit, and ensure sustainability.

ORGANIZATIONAL CULTURE

Organizational culture and tone at the top play a significant role in how involved the internal audit function is in reviewing and adding value to organizational governance. Culture embeds many intangibles, including soft controls. As referenced in the CBOK report, Promoting and Supporting Effective Organizational Governance, some of the soft controls that can be audited to help improve organizational governance include:

- Management and board competence, philosophy, and style.
- Mutual trust and openness.
- Strong leadership and a powerful vision.
- High performance and quality expectations.
- Shared values/understanding.
- High ethical standards.

These are areas in which most internal auditors lack audit experience and for which there are less formal training

TO COMMENT on this article, EMAIL the authors at sri.ramamoorti@theiia.org

and tools, making such culture audits much more challenging.

Periodic culture and ethics audits are one way to assess the ethical climate and control environment. Audits of incentives and compensation, as well as their alignment with the strategic plan and capital structure among key stakeholders, may also be helpful. For example, if the company is financed primarily through debt, the strategic plan should be more conservative and the executives' compensation should be more salary or bonus and less stock. Otherwise, there is an inherent conflict between what is desired and what is incentivized.

Clearly, the audit of soft controls embedded within organizational cultures consists of many intangibles that do not lend themselves to quantitative measurement and analysis. Accordingly, to be successful, internal auditors must possess soft skills, such as relationship-building acumen, political and cultural savvy, interpersonal communication abilities, diplomacy and tact, and an ability to read people and situations quickly and correctly.

ASSURANCE AND ADVISOR ROLES

Internal audit can undertake specific activities as part of their assurance and advisory work in supporting organizational governance (see "Internal Audit Activities for Organizational Governance Assurance and Consulting" on page 58). Many organizations

INTERNAL AUDIT ACTIVITIES FOR ORGANIZATIONAL GOVERNANCE ASSURANCE AND CONSULTING

Governance Assurance *(Helping the board and executive management use information with confidence.)*

1. Conduct comprehensive, enterprisewide governance audits with recommendations and an opinion about the overall governance system, enterprise risk management (ERM), and internal control effectiveness over time.
2. Address governance as a part of assurance services for other audits.
3. Perform strategy execution reviews to ascertain conformance with the agreed-upon strategic plan.
4. Provide assurance that ERM and systems of internal control are operating effectively (as a part of the overall governance processes).
5. Evaluate entity-level controls, which would be governance controls, such as tone at the top.
6. Ensure regular, frequent, open communication with the board and audit committee, including, formal private sessions without management present.
7. Mitigate information integrity risk, permitting the board and executive management to use decision-relevant information with confidence.

Governance Advisory Services *(Providing decision context, interpretation, and insight.)*

1. Conduct comprehensive, enterprisewide governance audits for the purpose of providing advisory services to improve governance structures and processes.
2. Address governance as a part of consulting services for other audits.
3. Communicate with board committees, such as the audit, nominating, governance, and risk management committees.
4. Educate the board/audit committee about best practices for governance.
5. Provide counsel to the board nominating committee and be involved in recruiting new board members.
6. Educate the board about developments and trends in the industry, such as new fraud risk assessment models, new technology tools (continuous monitoring), or new pronouncements.
7. Assist with board processes and activities (e.g., help with board self-evaluation processes, or help update the board's bylaws).

Only 8% of internal auditors report reviewing their organization's strategic plan, according to The IIA's CBOK 2015 Global Internal Audit Practitioner Survey.

enlist the assistance of internal audit to provide fraud risk awareness training, or help divisional units carry out control self-assessments by systematically conducting risk and control mapping in their specific context.

Assurance Services When providing assurance with respect to organizational governance, internal audit assesses the processes used to obtain relevant, reliable, and timely information for strategic decision-making. By providing assurance regarding the accuracy, consistency, and reliability of information, internal audit can help mitigate information for decision-making risk. Internal audit's work in assuring the quality of information used for decision-making allows the board and executive management to use information with confidence.

Advisory Services Internal audit provides consulting and advisory services to improve governance without assuming management responsibility. The types of consulting and advisory services that internal audit can offer include advising the board and executive management on decision-making processes, providing information on best practices, and offering interpretation/insight. Advisory services also encompass internal audit facilitating board and executive management awareness and education, instilling best practices in governance, and providing briefings on trending topics.

STRATEGIC GAP

All over the world, internal audit seems to take action more on risk indicators from perceived or actual weaknesses in internal controls over financial reporting, rather than those pertaining to strategic performance and operational risk factors, as indicated by the CBOK survey. This happens even though internal audit acknowledges the importance of strategic risk and believes that management and the board place a high priority on strategic risk. In other words, internal audit may not be meeting stakeholder expectations when it comes to strategy audits (i.e., how well is the planned and approved strategy being executed?).

A huge gap exists in terms of internal audit undertaking strategic reviews.

A huge gap exists in terms of internal audit undertaking comprehensive strategic reviews, even where a long-term strategic plan is in place. According to the CBOK survey, while approximately 50 percent or more of respondents' organizations around the world have a long-term strategic plan in place, internal audit only conducts strategic reviews 11 percent (South Asia) to 28 percent (Sub-Saharan Africa) of the time. Just as they do for general governance reviews, Sub-Saharan Africa and Middle East/North Africa have the highest levels of activity for reviews of strategy linked to performance.

Most surprising is that in North America, an average of 71 percent of respondents report having a long-term strategic plan in place, but only 8 percent of internal auditors report that they actually review the organization's strategic plan. The reasons for this gap in the "strategic plan existence vs. extensive strategic reviews" could be that they perform such reviews as part of other routine audits and make governance recommendations along the way rather than comprehensively, have immature or inexperienced internal audit functions that are not adequately supported or confident to carry out such strategic reviews, or strategic risks are given a low priority because they are not perceived to be a matter for concern. It could also be that managment does not support internal audit being in this space, that internal audit lacks support of the audit committee, or it doesn't have sufficient resources.

LOOKING FORWARD

In the future, more reliance will be placed on strategic and operational risk and performance data (forward looking) and on internal audit functions for more effective monitoring and governance oversight. Operational data provide a closer look at what is really happening with the business, but they also provide early warning signs of emerging risks that, if heeded, can prompt a critical and timely assessment of the business model and potentially preempt or avert business and governance failures. With internal audit's help, organizations can adapt to changing conditions in the marketplace, such as shifting consumer tastes and preferences and making needed course corrections to strategy, which can ensure continued growth and success.

SRIDHAR RAMAMOORTI, PHD, CIA, CPA, CFE, *is an associate professor of accountancy at Kennesaw State University in Georgia.*

ALAN N. SIEGFRIED, CIA, CPA, CRMA, CISA, *is assistant academic director, internal audit track, at the University of Maryland's Smith School of Business in Crofton.*

P. ALAN WHITE *is managing general partner at Quetzal GRC LLC in Austin, Texas.*

Governance Perspectives

BY JEFFREY RIDLEY EDITED BY MARK BRINKLEY

GOOD GOVERNANCE IS ALL ABOUT QUALITY

Five rules can be instrumental in achieving high standards of quality and governance.

Much has been written about the benefits of quality management: its measures and assurance in all types of organizations worldwide. The performance and success of hundreds of thousands of organizations and their operations around the world owe much to the development of, and compliance with, quality standards, total quality principles, quality auditing, and assurance frameworks.

Quality can be seen in the effectiveness of an organization's processes and the products and services it provides; seen by its customers, both internal and external, across all its supply chains; and by those who use its products and services. Quality is created by a focus on customer needs, leadership, teamwork, measurement, and a total commitment to continuous improvement.

As head of internal audit in a large manufacturing company in the 1980s, I was asked to join its Quality Council, established to drive a total commitment to register the company to the international quality systems standard ISO 9000 (The International Organization for Standardization has recently published updated principles for its ISO 9000 Quality management systems, www.iso.org). This responsibility introduced me to total quality management principles and the principles underpinning the standards for quality management systems. At the time, I developed and published five quality rules to guide my learning (see "Five Quality Rules" on page 63). These rules have been a guide for me in understanding how to achieve high standards of quality and also the importance of achieving them in all that makes up good governance.

Associations of quality professionals around the world recognize these rules to be fundamental for a commitment to quality. They can be seen in their visions and missions, their knowledge base, competency frameworks, training, and qualifications. Go to the Chartered Quality Institute website (www.quality.org), or the quality institute in your own country, and compare these rules with its strategic objectives. World Quality Day, Nov. 10, 2016, adopted the theme "Making Operational Governance Count," sending the message that good governance is all about quality.

Quality, like good governance, is an assessor of risk and a driver of control activities. It requires high levels of accountability, integrity, and openness in how it is achieved and perceived by an organization's stakeholders. Like good governance, trust is at the core of all quality systems and quality auditing. Quality assurance is a must for every type of activity, service, and product, both for the supplier and the customer. It is a requirement for the efficiency, effectiveness,

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

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

FIVE QUALITY RULES

CUSTOMER FOCUS
- All customers are different; their satisfaction is paramount.
- Focus on both internal and external customers, primary and secondary.
- View all customers as partners in your supply chains.
- Understand all your customers' needs.
- Aim for customer delight, not just satisfaction, at all times.
- Do not ignore customer complaints.

MANAGEMENT LEADERSHIP
- Organize for quality.
- Establish a clear and motivating vision understood by everyone.
- Identify your key success factors and build these into a clear mission statement.
- Provide the right structures, methods, and resources for quality achievement.
- Communicate well at all levels, both in clarity and timeliness.
- Give high visibility to your quality policy.

TEAMWORK
- Recognize and encourage the power of teams.
- Develop teams across the entire supply chain, internal and external.
- Interlock all teams at operation, function, and cross function levels.
- Reinforce and reward teams for success.
- Teach teams to focus on your vision and mission statements.
- Delegate responsibility to teams to take action.

MEASUREMENT
- If it cannot be measured, it cannot be improved.
- Measure by statistics—do not inspect.
- Establish measures in all processes, across all supply chains, with high visibility.
- Relate all measures to your vision and mission statements.
- Focus measures on customers, both internal and external.
- Take prompt corrective action on all measurements.

TOTAL COMMITMENT TO CONTINUOUS IMPROVEMENT
- Look for problems, develop solutions, and train.
- Create a learning organization with a constant commitment to improve.
- Encourage a constant and continuous search for excellence.
- Be creative—look for paradigm shifts.
- Benchmark, internally and externally.
- Verify the success of change.

and economy of every organization in the performance of its activities and achievement of its vision and missions. It must always be present in the values the organization promotes for itself and in its services and products.

In my five quality rules, replace the word "customer" with "stakeholder" and "quality" with "good governance" to relate each of the rules to the policies and regulations for good governance. Good governance is all about quality, and quality is all about good governance — both for organizations and in the audit, inspection, and compliance services they use.

These rules can be found in the values of good corporate governance. Quality achievement is required in each of the recently redeveloped and published G20/Organisation for Economic Co-operation and Development corporate governance principles. It can be found in corporate governance codes everywhere, and in many standards and laws. It is a requirement for all audit practices. Quality achievement and monitoring also is seen by many as part of the second line of defense in achieving good risk management and control. The IIA promotes this in The Three Lines of Defense for Effective Risk Management and Control. Requiring collaboration at the second line of defense with other monitoring activities is fundamental to good governance. In fact, quality should be more than a collaborator in an organization's second or third lines of defense; quality should be an attack.

Audit committees have a key role in monitoring governance in each of the three lines of defense throughout the organization. This monitoring should include the standard of quality in the performance of all those it relies upon for assurance as a defense. Audit committees should also recognize the importance of quality, not just as a defense, but also as an attack on inefficiency, ineffectiveness, and waste in all its forms. la

JEFFREY RIDLEY, CIA, *is visiting professor of auditing at London South Bank University and visiting professor of corporate governance assurance at the University of Lincoln, England.*

ENGAGE AND CONNECT GLOBALLY

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

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

www.theiia.org/advertise

75TH ANNIVERSARY 1941-2016

The Institute of Internal Auditors

2016-1116

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

BY J. MICHAEL JACKA

THE BEAM IN INTERNAL AUDIT'S EYE

Before they can establish credibility with stakeholders, practitioners must first get their own house in order.

Imagine you have just completed an audit. The details are not important. All you need to know is that the department is composed of professionals—individuals whose jobs require them to be self-directed, critical thinkers who understand the business and communicate effectively.

You have identified two potential problems. First, every action taken by each professional in the department is subject to review by that individual's superior. Subsequent to that review, the department conducts a second set of reviews to ensure the work is correct and that the first review was completed.

Second, considerable rework occurs before the department publishes any results. A disproportionate amount of time is scheduled on all projects simply for the publication process. Moreover, the rework results in significant delivery delays.

Anyone with a modicum of internal audit skills should see these processes are the result of an overemphasis on controls. The first question an auditor should ask is whether the cost of those controls matches the cost of the related risk. Next, why not streamline the process by removing some (if not all) of the reviews? And third, what is the root cause of the constant rewriting?

Have you guessed where I'm headed on this one? Procedurally, how much of the audit documentation you create has to undergo a first and second round of approvals? (Hint: The answer is probably all of it.) How many rewrites did your last audit report go through? (Hint: If you answered fewer than five, I'm not sure I believe you.)

It is internal audit's job to evaluate the efficiency and effectiveness of processes, ensure risks are managed appropriately, and ultimately, help the organization achieve its objectives. We expend enormous foot-pounds of energy toward that end. And yet, how much effort do we put into self-analysis? How much time do we spend auditing ourselves?

Are you able to explain how the internal audit department's objectives align with the organization's objectives? Can you articulate the risks to the audit department's achievement of its objectives? Can you identify the controls that ensure those risks are managed appropriately? And perhaps most importantly, when was the last time you took a good, hard look at your processes to see where gaps might exist or (much more likely) where those process might be overcontrolled?

If internal audit wants to ensure true credibility with its stakeholders, we must look inward—we must evaluate our own policies and procedures. And in so doing, we will surely see that we are as guilty of reportable issues as anyone we audit. Quite simply, internal audit must cast the beam from its own eye before it can see clearly enough to cast out the mote from the client's eye. 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

MANAGING TALENT TO ADDRESS EMERGING RISKS

Auditors need to shift their attention from traditional ways of addressing risk to a bigger picture focus.

BRIAN CHRISTENSEN, executive vice president, Global Internal Audit, Protiviti

BILL WATTS, partner and leader of Risk Global Thought Leadership, Crowe Horwath

What are the biggest risks internal auditors are not currently auditing?

WATTS 1) Technology risk—increasing complexities of cyber threats and the possibility of security breaches, as well as the rapidly evolving Internet of Things; 2) geopolitical and economic risk—fluctuations in oil and other commodity prices, geopolitical conflict, and the rise and fall of emerging markets; 3) evolving corporate reporting—regulators worldwide are looking for more narrative in corporate reporting and more details on the significance of nonfinancial risks; and 4) more complex domestic and global regulations. Companies also need to be aware of emerging global regulatory trends that could be enacted in the U.S. or affect their operations overseas. Examples include the proposed revenue recognition standards and executive compensation disclosure.

CHRISTENSEN The internal audit profession is embarking on new and exciting territory for meeting the expectations of stakeholders in addressing nontraditional risks. Historical bias or repeating the past often results in an audit program focused on financial or operational controls. These remain critical components of a standard risk approach, but they may not address the most relevant or timely concerns. Qualitative and abstract topics such as culture, innovation, digitalization, and geopolitical risk are current examples of audit hot topics. These may not be the ordinary top-of-mind audit risks; however, they are relevant to the boardroom and need to be addressed to demonstrate the value of internal audit. Auditors should embrace the opportunity to measure and monitor these exposures.

How can CAEs quickly bring their teams up to speed on these risks?

CHRISTENSEN Internal audit teams must understand that macro-environmental business, industry, and company risks influence the audit universe. Each of these factors must be considered in assessing and executing audit plans. Internal auditors must be astute in monitoring and gathering the necessary data points to direct their actions. The CAE can be a leader in disseminating facts, but more importantly, teaching team members how to mine for information improves team performance.

WATTS Internal auditors need to pay closer attention to external risks of the organization based on how business is conducted, and recognize the impacts on the organization's strategy and performance. Auditors can do this by: acquiring the technical skills to audit new reality and risks; knowing and maintaining an understanding of industry and risks—competitive landscape, market drivers, and applicable regulations; using technology and software

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

MORE VISIT our Mobile app + InternalAuditor.org to watch a video discussion on talent management at Citigroup.

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

tools that can render internal audit's skills and knowledge more effective; and getting involved in operation group meetings and projects to better understand how the organization is changing.

What is a longer term strategy for ensuring auditors are prepared to address emerging risks?

WATTS Auditors need to stay agile, relevant, and valuable by shifting focus from traditional ways of addressing risk to a future thinking/bigger picture focus. This can be accomplished by aligning risk assessments to include market trends, research, and development at the organization, and studying competitor changes. Change must be transformational, not just surface dressing, and will require bold moves to break down old paradigms and create a new model for the future. Internal audit must be proactive versus reactive and embrace change while it is occurring instead of after the fact.

CHRISTENSEN Internal auditors must appreciate that continuous and rigorous education is critical for long-term success in addressing emerging risks. Time and experience are highly valuable to the core learnings in a career. Additionally, exposure to new and emerging ideas and concepts makes the internal auditor relevant, valuable, and capable of addressing the latest trends and their impact on an organization.

What advice do you have for CAEs struggling to determine the right mix of specialized expertise and audit generalists?

CHRISTENSEN All business leaders are tasked with the challenge to build, buy, or rent the skills necessary to achieve a task. The CAE is not immune to this decision tree. The specific facts and circumstances will dictate the approach and level needed and which category. We live in a knowledge-based era, and CAEs must measure the return on their investments and the value to the organization. Specialized IT skills are a great example. Does the value come from seeing many of the same thing or only seeing one thing for an extended period? Different facts may result in different outcomes. The CAE must apply the decision tree and be flexible to maximizing the value equation.

WATTS It is not so much the balance vs. the evolving of the type of auditors you must recruit and develop in your group. You can no longer be one or the other, but must have the versatility to be both in certain areas. Auditors need to be broad in their experience, but also constantly gain knowledge in specialized skills to help add value. The future internal auditor will need to have good soft skills and process and operations knowledge, and not be trained only in traditional methods. Look for individuals with varied backgrounds who have a skill for problem solving and interest in areas that are new to the business world, such as rapidly changing technology usage, data analytics, and mathematics.

How can hiring managers ensure their audit team members represent a good cultural fit for the organization?

WATTS This is the challenge for organizations as the workforce becomes more diverse. You must know not only your organization's culture, but also the internal audit group's unique culture. It is important that internal audit communicates and discusses these two areas with every candidate to ensure a strong fit in both environments.

CHRISTENSEN A common theme resonating with boards and management is that internal auditors need to be strong communicators with organizational insight. This might be interpreted to mean internal auditors cannot be lost on the audit trail hiding behind the technical mechanics. Stakeholders want interaction that is a cultural fit. Hiring managers should look at the entire work of the candidate. The technical and educational experiences are often the base level, but what about the broader accomplishments? Can the candidate demonstrate a service mentality, team orientation, adaptability, and similar qualitative characteristics? Life skills are developed in many areas, and we all need to hone these traits. Hiring managers will find these skills will highly correlate to candidates with the best cultural fit.

What is one key tip you would offer CAEs who are developing a talent management strategy?

CHRISTENSEN CAE success is dependent on the robustness of a talent management strategy. People want to be inspired and led. They seek leaders who can show them the way. This is not a once-a-month activity or something that can be relegated to someone else. The CAE must be the coach, mentor, teacher, and leader, every day, 24/7. Be a role model to your people and you will be rewarded in ways never imagined.

WATTS Blow up the traditional strategy and think outside the box. Today's environment is changing so rapidly that the needs and skills can't keep up. Think about the end results that are desired in internal audit, and build back to what skills and people you need, not for today, but for what is envisioned over the next three to five years. Be bold and challenge yourself and your organization to take chances on hiring different skill sets and experiences to meet the organization's risk based on where it is headed, not where it is today. ia

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

BY ADAM P. KRICK

JUST A FEW MORE QUESTIONS

The final audit report should not mark the end of an engagement.

Internal auditors often approach their assignments with a one-sided focus. Given all of the effort and resources devoted to completing engagements, practitioners naturally pay close attention to their own findings, recommendations, and message delivery. But it's just as important for auditors to hear from clients on the outcome of an engagement, particularly when it's in the form of constructive criticism. At a certain point, auditors need to put away the reports, turn off the PowerPoint slides, and open their ears to feedback from the stakeholders they serve.

Communication, of course, is a two-way street. Auditors cannot operate in a vacuum or perform their work effectively without gauging clients' responses to the audit process. Opening up the process to feedback can only lead to insight and improvement, and it is essential to understanding the client experience.

Neither clients nor the auditor should be prone to the mind-set that an engagement ends when the final audit report is issued. On the contrary, an important information-gathering tool follows behind the audit report that simultaneously takes the pulse of recently audited clients and sets the foundation for future audits: the post-audit survey. Regardless of the delivery method—online, paper-based, or verbal—this opportunity for direct feedback can be a priceless resource.

While clients often are more inclined to share negative feedback, positive feedback should also be captured and can be just as useful. When a client expresses appreciation during an engagement, auditors can suggest the survey during the exit meeting as an appropriate outlet for such accolades. The process isn't merely about notifying the chief audit executive of a job well done—post-audit surveys gather tangible data points from which the auditors can learn and the audit process may improve.

As with any survey, constituents may choose not to participate—and they should not be forced to. Moreover, regardless of whether feedback is positive or negative, the success of a survey should be measured not by the quantity of responses but by the quality of feedback from open-ended questions. Open-ended comments often become the building blocks of improved audit processes, leading to greater efficiency, better communication, and more productive engagements.

The auditor's ultimate responsibility is not to seek out compliments on job performance or audit quality, nor is it to invite denunciation or disparagement. Constructive criticism provided after the issuance of the final report has great potential to fuel positive improvements, recognize success or shortcomings, or simply convey appreciation for a courteous, well-rounded, and insightful audit that added value. While the post-audit survey can be easy to overlook when planning an engagement, auditors should always include this important tool—particularly because it involves the simple task of asking just a few more questions. IA

ADAM P. KRICK, CIA, CFSA, *is a lead auditor at Customers Bancorp in Wyomissing, Pa.*

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

There's a Center For You

Stay ahead of the curve on the issues that matter most to you and your stakeholders.

Audit Executive Center®

Environmental Health & Safety Audit Center

Financial Services™ Audit Center

ACGA® American Center for Government Auditing

Canadian Public Sector Audit Centre

Learn more at
www.theiia.org/SpecialtyCenters

75th Anniversary 1941-2016

The Institute of Internal Auditors

2016-0776

Wolters Kluwer

When you have to be right

TeamMate+

The future is here

Better tools. Better team. Better audit.

Register for a demo at
TeamMateSolutions.com/Demo

See it in person in March at
IIA GAM in Orlando, Florida

PRINCIPAL PARTNER